SEPPmail

Version 7.0.2

User Manual
with Ruleset

SEPPmail AG
Industriestrasse 7
CH-5432 Neuenhof

+41 56 648 28 38 fon
+41 56 648 28 39 fax
info@seppmail.ch mail

www.seppmail.ch

Inhaltsverzeichnis

Part I Foreword 7

Part II Introduction 8

1 Secure email communication through encryption 9

2 Digital email signatures 11

3 Central Business Email Disclaimer 11

4 Email content check by Virus, Spam and Phishing Protection (VSPP) 12

5 Compatibility with other secure email systems 12

6 Remote administration using a web portal 12

Part III Commissioning of the Secure Email Gateway Appliance 13

1 Before starting 13

2 Integration of the appliance in your email environment (default configuration) 13

3 Required information for commissioning 15

4 Connecting SEPPmail appliance 17

5 Setting up Firewall / Router 17

6 Network settings and System Registration 19

Setting up installation PC 19
Logging in as Administrator 20
Network settings of the SEPPmail appliance 20
Assigning host and domain names 21
Checking the network configuration 21
Bringing the system to the latest version 22
Registering the system 22

7 Important safety measures 23

Changing Administrator Password 23
Setting the HTTPS protocol for secure access to the system 23
Creating backup user 23

8 Next steps 24

Converting email data flow 24
Using email clients 26

Part IV Microsoft Outlook Add-In 27

1 Introduction 27

2 System requirements 27

3 Download 28

4 Installation 28

Installation with a user interface 29

© 2014 SEPPmail AG

Installation without a user interface ... 31
5...Uninstallation of Microsoft Outlook Add-In ... 32
6...Registry entries of the Microsoft Outlook Add-In ... 33
HKEY_LOCAL_MACHINE ... 33
HKEY_CURRENT_USER ... 35
7...Sending emails ... 36

Part V SEPPmail - IronPort connection 37

Part VI Reference of the menu items 40

1...Configuration Overview ... 40
2..."Login" menu item ... 41
3..."Home" menu item ... 42
4..."System" menu item ... 44
Overview of "System" menu item ... 44
Forwarding email logs to a central syslog server ... 50
Setting the date and time and setting up NTP synchronization ... 50
Enabling SNMP ... 51
5...Menu item "Mail System" ... 52
Overview of the "Mail System" menu item ... 52
Setting up for managing email domains ... 58
Controlling outgoing email traffic ... 58
Setting up per domain TLS encryption ... 58
SMTP settings ... 61
Mail Relaying ... 61
Anti-spam settings ... 62
Managing Blacklists / Whitelists ... 63
6..."Mail Processing" menu item ... 65
GINA web mail interface ... 65
Creating GINA domains ... 66
Deleting GINA domains ... 66
Managing GINA Domains ... 66
Managing GINA Layout ... 72
Managing GINA language support ... 75
GINA self registration through web mail portal ... 78
Managing GINA Accounts ... 79
GINA Self Service Password Management ... 80
GINA internal encryption ... 80
GINA S/MIME and PGP key search via GINA Portal ... 81
Managing rules for the processing of GINA messages ... 82
Managing GINA SMS password transmission ... 84
Managing Disclaimer ... 87
Managing email templates (Templates) ... 88
Managing rulesets ... 89
Viewing and loading rulesets ... 102
.7..."SSL" menu item ... 103
Creating self SSL device certificate ... 103
Requesting SSL device certificate from a public CA ... 105
Using existing SSL Device Certificate ... 106
Backing up SSL device Certificate ... 106
.8..."CA" menu item ... 108

© 2014 SEPPmail AG

Managing internal CA settings ... 108
Setting up CA certificate ... 109
Securing CA certificate ... 109
Setting up a connection to the external CA S-Trust ... 109
Setting up a connection to the external CA Signtrust ... 110
Setting up a connection to the external CA SwissSign ... 110
.9..."Administration" menu item ... 112
Registering SEPPmail appliance ... 112
Importing license file ... 112
Checking appliance for available updates ... 113
Backup and restore settings of the appliance ... 114
Rebooting or shutting down the appliance ... 115
Reseting the appliance to factory settings ... 116
Import existing user or key ... 116
Establishing Outgoing Support Connection ... 117
10..."Cluster" menu item ... 118
General ... 118
High Availability Cluster ... 118
Load Balancing Cluster ... 121
Geo Cluster ... 127
Frontend-Backend Cluster ... 128
Setting up a Cluster Configuration ... 129
Overview ... 131
Safety notes ... 131
Configuration of the VMware ESX environment ... 133
Setting up the basic settings of a SEPPmail system ... 134
Setting up the SEPPmail cluster systems ... 134
Downloading cluster identification ... 134
Setting up SEPPmail cluster ... 136
Setting up High Availability Cluster ... 139
Setting up Load Balancing cluster ... 141
Setting up Geo Cluster ... 143
Setting up Frontend-Backend cluster ... 143
11..."Logs" menu item ... 145
Viewing email messages in the queue ... 147
12..."Statistics" menu item ... 148
13..."Users" menu item ... 151
Overview of the "Users" menu item ... 151
Creating internal user ... 151
Managing Internal Users ... 152
14..."Groups" menu item ... 156
Overview of the "Groups" menu item ... 156
Creating groups ... 158
Managing groups ... 158
Assigning and removing users ... 158
15..."GINA accounts" menu item ... 160
Overview of the "GINA accounts" menu item ... 160
Blocking GINA user accounts ... 162
Removing GINA user accounts ... 162
Managing GINA user accounts ... 162
16..."PGP public keys" menu item ... 166
Overview of the "PGP public keys" menu item ... 166

© 2014 SEPPmail AG

Importing OpenPGP key ... 166
Downloading or deleting OpenPGP key ... 166
17. "X.509 Certificates" menu item ... 167
Overview of the "X.509 Certificates" menu item ... 167
Importing S/MIME user certificate ... 167
Downloading or deleting S/MIME user certificate ... 168
18. "X.509 Root Certificates" menu item ... 169
Overview of the "X.509 Root Certificates" menu item ... 169
Importing X.509 root certificates ... 170
Downloading and deleting X.509 root certificates ... 170
Trusting X.509 root certificates ... 171
Automatically importing X.509 root certificates ... 171
19. "Domain keys" menu item ... 172
Overview of the "Domain Keys" menu item ... 172
Importing OpenPGP domain keys ... 173
Downloading or deleting OpenPGP domain keys ... 173
Importing S/MIME domain keys ... 174
Downloading or deleting S/MIME domain keys ... 174
Managing domain keys ... 174
20. "Customers" menu item ... 175
Creating new customers ... 176
Managing existing customers ... 176
Deleting existing customers ... 178
Part VII Reference of the set of rules statements 179
.1. Control structures - if/else statements ... 179
.2. General commands ... 180
add_rcpt() ... 180
authenticated() ... 181
compare() ... 182
compareattr() ... 184
comparebody() ... 185
disclaimer() ... 185
from_managed_domain() ... 186
incoming() ... 187
log() ... 188
logheader() ... 189
normalize_header() ... 190
notify() ... 191
replace_rcpt() ... 192
replace_sender() ... 193
rmatch() ... 194
rmatchsplit() ... 195
rmheader() ... 196
setheader() ... 197
logsubject() ... 198
tagsubject() ... 198
.3. User management commands ... 200
createaccount() ... 200
member_of() ... 201
setuserattr() ... 201
.4. Certificate management commands ... 203

© 2014 SEPPmail AG

attachpgpkey() ... 203
has_smime_key() ... 203
smime_create_key() ... 203
smime_revoke_keys() ... 204
swisssign_create_key() ... 204
.5. Message handling commands ... 206
archive() ... 206
bounce() ... 206
deliver() ... 207
drop() ... 208
reprocess() ... 209
.6. Encryption and decryption commands ... 211
decrypt_pgp() ... 211
decrypt_domain_pgp() ... 211
domain_pgp_keys_avail() ... 211
decrypt_smime() ... 212
decrypt_domain_smime() ... 212
domain_smime_keys_avail() ... 212
delete_smime_sig() ... 213
encrypt_pgp() ... 213
encrypt_domain_pgp() ... 214
encrypt_smime() ... 215
encrypt_domain_smime() ... 215
encrypt_webmail() ... 216
pgp_encrypted() ... 216
pgp_keys_avail() ... 217
pgp_secret_keys_avail() ... 217
smime_keys_avail() ... 217
sign_smime() ... 218
smime_signed() ... 218
smime_encrypted() ... 219
validate_smime_sig() ... 219
webmail_keys_avail() ... 220
webmail_keys_gen() ... 220
pack_mail() ... 221
unpack_mail() ... 222
.7. LDAP commands (access to external sources) ... 223
ldap_compare() ... 223
ldap_read ... 224
ldap_getcerts() ... 225
ldap_getpgpkeys() ... 226
.8. Content management commands ... 228
iscalendar() ... 228
isspam() ... 228
partoftype() ... 229
vscan() ... 230
.9. File types ... 231
List of file types ... 231
Groups of file types ... 233

© 2014 SEPPmail AG

1 Foreword

The SEPPmail AG reserves the right to make changes to the contents of this document, at any time and without notice. Unless otherwise noted, names and dates of people or companies used in this document as application examples, are fictitious. The preparation of an appropriate number of copies of this document is permitted, but only for internal use. This document may not be copied or reproduced for other purposes; either partially or completely, by non-electronic, mechanical or any other means, except with expressly written approval of the SEPPmail AG.

The contents of this document may have been altered, if you did not get it directly from the SEPPmail AG. Although this document was produced with the greatest care, SEPPmail AG assumes no responsibility for any errors or omissions. The use of this document contains the approval for its use without defect guarantee and without any warranties. Any use of the information contained herein at your own risk.

PGP and Pretty Good Privacy are registered trademarks of PGP Corporation, valid in the U.S. and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc., valid in the U.S. and other countries. UNIX is a registered trademark under the disposal of the X/Open Company, valid in the U.S. and other countries. Microsoft, Internet Explorer, Windows, Windows NT, Windows 2000 and Windows XP are either registered trademarks or trademarks of Microsoft Corporation, valid in the U.S. and other countries. Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation, valid in the U.S. and other countries. Any and all other trademarks listed herein are the property of their respective owners and are used here with no intention of trademark infringement.

OpenSSL is an application, that is distributed under an Apache-style license (www.openssl.org).
OpenBSD is an operating system, which is sold under the Berkeley Copyright (www.openbsd.org).
GnuPG is software, that is distributed under the GNU Public License (www.gnupg.org).
The Apache web server and Apache Tomcat are developed under the Apache Software Foundation Copyright (www.apache.org).

References to commercial products, processes or services, by naming the product or the manufacturer's name or in any other way, are not necessarily the same as an endorsement, recommendation, or favoring by the SEPPmail AG.

Import, export and use of these and other cryptographic products may be restricted by law.

The author views expressed and opinions in this document do not necessarily express those of SEPPmail AG and may not be used for the advertising purposes or product recommendation. References to Internet addresses have been checked thoroughly before printing. Due to the constant change of Internet content, SEPPmail AG cannot guarantee the existence and contents of the specified assumed sources. If you find broken links in this guide, please tell us about it, stating the links concerned and the version number of this instruction to the address info@seppmail.ch.

Print: August 2014, CH-5432 Neuenhof

© 2014 SEPPmail AG

2 Introduction

Welcome to the secure email solution SEPPmail

This manual supports you in SEPPmail installation and serves as a reference of the various configuration aspects. It is divided into the following three parts:

Part I	The first part consists of an introduction to the product. The operation and important product characteristics of the SEPPmail appliance are described here.
Part II	The second part explains how to bring the secure email Gateway SEPPmail in operation. This includes the integration of the appliance into your network and setting up your email and network environment.
Part III	The third and last part contains, in the first chapter, an overview of the various configuration options. The remaining chapters describe configuration and administration steps of the individual menu items in detail. The outline is intended for easy orientation to the menu structure of the web administration portal.

We wish you successful installation.

© 2014 SEPPmail AG

2.1 Secure email communication through encryption

SEPPmailrelies on various standardized encryption methods and offers the highest level of security for different communication partners. This chapter describes the methods that can be used.

The Secure Email Gateway Appliance SEPPmail decrypts incoming emails automatically. The process is completely transparent to the email recipients. They receive emails unencrypted in the mailbox and read them as before, without any additional effort.

Incoming emails can be provided with a digital signature. Part of this signature is the public S/MIME certificate of the sender. In order to minimize the administrative burden, the SEPPmail appliance stores this S/MIME certificates automatically and uses them for S/MIME email encryption for respective communication partner.

For the safe emailing, the SEPPmail appliance selects from the following 5 methods the best possible for the recipients:

1. GINA technology

The GINA encryption technology contains a patented process. Here email messages are not cached until pick-up, as usually in other webmail methods, but delivered fully encrypted to the recipient. There they are stored in their mailbox (e.g. Outlook). Emails are protected in this process against phishing attacks, because besides the password, also the encrypted email itself is required for successful access from the recipient's mailbox.

A GINAmessage contains the message in encrypted form, as a file attachment. The recipient retrieves the message by opening the encrypted file system on the local web browser. This is then processed via secure SSL connection (HTTPS) and transferred to the SEPPmail appliance of the sender and decrypted there and displayed after entering a user password. By entering the password, the recipient's identity is checked at each poll. In contrast to the traditional emailing, email deliveries can be ascertained, thanks to the correct authentication. The figure below shows an example of a GINA message.

test - Nachricht (HTML)
Nachricht
Entwicklertools
Antworten
Allen antworten
Weiterleiten
Löschen
In Ordner verschieben
Regel erstellen
Andere Aktionen
Absender sperren
Listen sicherer Adressen
Keine Junk-E-Mail
Kategorisieren
Nachverfolgung
Als ungelesen markieren
Suchen
Antworten
Aktionen
Junk-E-Mail
Optionen
Von: u3sec [andreas.berger@webinit.net]
Gesendet: Fr 05.03.2010 19:59
An: andy@test2.swisssecure.ch
Cc:
Betreff: test
Nachricht
secure-email.html (6 KB)
Sie haben ein verschlüsseltes E-Mail erhalten.
Sie können die Nachricht anschauen, indem Sie die angefügte Dateianlage in einem Internetbrowser (z. B. Internet Explorer) öffnen und das entsprechende Passwort eingeben. Je nach Dateigrösse und Internetverbindung kann es eine Weile dauern, bis das Anmeldefenster angezeigt wird.
Sollte dies das erste verschlüsseltes E-Mail sein, das sie von uns erhalten, wird Ihnen das Passwort vom Absender mitgeteilt.
Sie können das Passwort nach Ihren Wünschen ändern. Zukünftige Emails, die Sie von uns erhalten, öffnen Sie immer mit demselben Passwort.
Sie haben bereits ein Passwort erhalten, dieses jedoch vergessen? Setzen Sie sich bitte mit dem Absender dieses E-Mails in Verbindung.
Wenn Sie das E-mail im Internetbrowser beantworten, wird Ihre Nachricht gleich verschlüsselt zurück gesendet.

Vous avez reçu un E-mail chiffré.
Vous pouvez voir le message, en ouvrant le fichier en pièce jointe dans un navigateur Internet (ex. Internet Explorer) et
Example of a GINA message

© 2014 SEPPmail AG

2. Fully automatic email domain encryption between all SEPPmail appliances

The SEPPmail appliance offers you the opportunity to permanently encrypt the email traffic between multiple email domains. The only condition is, that the communication partners via each have a SEPPmail appliance. All messages are automatically encrypted and decrypted between the systems. With this method, so-called domain certificates i.e. domain keys can be used.

3. S/MIME user encryption

The process of encryption using S/MIME is based on public and private keys. With public keys, the emails are encrypted and can subsequently only be decrypted with the associated private keys. Thanks to the central processing, this is done automatically, if the corresponding S/MIME user certificates exists on the SEPPmail appliance. These can be created on the SEPPmail appliance itself or issued by a public certificate provider. In both cases, the certificates can be automatically created. The SEPPmail appliance supports, for this purpose, various interfaces to public certificate providers.

4. OpenPGP user encryption

OpenPGP works on the same basic principle as S/MIME. The OpenPGP keys are managed on the SEPPmail appliance and email is automatically encrypted and decrypted, if the required keying material is correspondingly available. Unlike S/MIME keys, with OpenPGP the keys are always self-generated and not issued by different public CAs.

5. TLS/SSL transport encryption

TLS/SSL provides additional security and complements the encryption methods described so far. The communication between the SEPPmail appliances and other email servers is set up in the default configuration always over a TLS/SSL secure channel, if the other party supports this. Also, TLS/SSL is used in the above-described email domain encryption between several SEPPmail appliances.

© 2014 SEPPmail AG

2.2 Digital email signatures

Use of digital email signatures ensures the binding email communication, in which the verification of the authenticity of a message can be done. It is thus ensured, that a message arrives unchanged to the recipient and also that the sender displayed is the actual sender.

The secure email gateway SEPPmail can either sign your emails with user or company certificates. The two methods are described briefly below:

Digital email signature with a user certificate

The signing of emails with an S/MIME user certificate allows the recipient to verify the authenticity of the email through the email client. This allows to ensure, that the sender is authentic and that the email has not been changed during and after sending. This method requires a separate S/MIME certificate for each email sender.

We recommend the use of certificates issued by a public certificate provider. You can automate this process by using one of the SEPPmail appliance's built-in CA connectors to various official certification bodies. The connection of the SEPPmail appliance to public certificate providers enables you with a fully automated issuing of certificates, without maintenance expense.

Alternatively, emails can also be signed in email client of each sender. The secure email gateway SEPPmail will then just encrypt these emails. Many S/MIME certificates are suitable both for signing and for encryption. It may therefore be useful to install the additional certificates in the SEPPmail appliance. This allows email messages to be automatically decrypted with the corresponding certificates.

Digital email signature with a company certificate

The signing of emails with an S/MIME company certificate serves the same purpose as the signing with an S/MIME user certificate. However, in this variant only a single certificate is required.

Since S/MIME certificates are generally only valid for one email sender address, all outgoing emails get the same (technical) sender. Emails appear at the recipient always with the same email address, but with the correct user name. Automatic recording of contacts and their email addresses no longer function as expected at the recipient. Likewise, difficulties are to be expected at other locations. Consequently, there is a risk, for example, that all your corporate emails will be rejected, if the used sender address is incorrectly classified as SPAM at the recipient.

2.3 Central Business Email Disclaimer

The Secure Email Gateway SEPPmail can complement your emails with a corporate email disclaimer. It supports disclaimer in text or HTML format.

Take advantage of the central company disclaimer to attach a single text or particulars, such as address and business owner to all emails.

Example in text format:

```
Company Ltd - Sample street 1, 1234 Sample city - www.mycompany.ch
```

© 2014 SEPPmail AG

2.4 Email content check by Virus, Spam and Phishing Protection (VSPP)

SEPPmail Protection Pack (Virus, Spam and Phishing Protection) is available as an option and protects you from spam (unsolicited emails), viruses (malicious emails) and phishing email messages (fraudulent emails).

The antivirus component continuously updates its virus definitions and automatically performs virus scans of your emails.

SPAM emails are effectively controlled by the integrated and easy to configure SPAM filters. This is based on the combination of different filtering techniques, such as Greylisting, Blacklisting, Bayesian filtering and SMTP protocol checks.

Phishing attacks are prevented by GINA messages, in which the recipient requires both the encrypting of the message itself, as well as a password to retrieve it.

Note, when used with existing anti-virus systems

The SEPPmail appliance can also be used with existing anti-virus systems. Note, however, that SEPPmail sends/receives the email encrypted.

To check emails for viruses, they must be available in unencrypted form. You should therefore run the virus check after decryption through your internal network (e.g. on your internal email server), if you want to continue to use your existing antivirus product.

2.5 Compatibility with other secure email systems

Because of the central email processing and key management, SEPPmail can be transparently integrated into your email infrastructure. All recognized and secure default encryption techniques are implemented. The compatibility with the common secure email systems is thus ensured and the installation of additional software components is omitted.

For recipients who do not have S/MIME certificate or OpenPGP keys, the GINA technology can be used for secure email transmission.

2.6 Remote administration using a web portal

All administrative capabilities of the SEPPmail secure email gateway are available via a web browser based configuration interface. The connection between the web browser and the SEPPmail secure email gateway is also encrypted (HTTPS).

© 2014 SEPPmail AG

3 Commissioning of the Secure Email Gateway Appliance

3.1 Before starting

Please check the package contents for completeness. The delivery comprises:

Quantity	Description
1	SEPPmail hardware appliance i.e. SEPPmail virtual appliance for VMware ESX or Microsoft Hyper-V server
1	Quick Install Guide
1	Power cord (240V)

If your delivery appears to be incomplete, or should any problems, or questions arise during installation of the SEPPmail appliance, please contact SEPPmail or your SEPPmail dealer.

A list of the contact details of the respective dealers can be found at the website of SEPPmail AG - http://www.seppmail.ch.

3.2 Integration of the appliance in your email environment (default configuration)

In this chapter, a simple scenario is described, in which the SEPPmail appliance accepts external emails directly from the Internet and sends internal emails externally to the Internet. Depending on the design of your email infrastructure, other email servers or gateways may appear in the email data flow.

In this scenario, SEPPmail is installed as an SMTP gateway between the Internet and your internal email server. This email data flow changes in the following two essential points:

1. Emails from the Internet are no longer directly sent to your internal email server, but (new) to the SEPPmail appliance.

2. Your email server no longer sends its emails directly to the Internet, but (new) to the SEPPmail appliance. The SEPPmail appliance thus assumes a smart host function.

© 2014 SEPPmail AG

The email infrastructure for the described structure is shown in the figure below.

Typical structure of an email infrastructure with a SEPPmail appliance

© 2014 SEPPmail AG

3.3 Required information for commissioning

It is recommended to compile the following information in your email environment before beginning the commissioning:

Required information	Your information
Public DNS entry or public IP address of the appliance*: This is the name or the IP address at which your SEPPmail appliance will be accessible on the Internet.	
Internal IP address of the appliance: The internal IP address and subnet mask, under which the SEPPmail appliance will be accessible in your internal network.	
Host name of the appliance: A freely selectable name of your host SEPPmail appliance, e.g. secureemailgateway. This is often specified in the DNS server.	
Internal domain in which the SEPPmail appliance is located: Examples: yourfirm.local or yourdomain.uk etc.	
Default Gateway IP Address: This is the default gateway IP address of your firewall or your router, through which the SEPPmail appliance can connect to the Internet.	
DNS Server: You can enter up to three DNS server IP addresses. These can be both internal as well as external DNS servers. Internal DNS servers must forward requests for external addresses accordingly.	
Host name or IP address of the existing internal email server: Host name or IP address under which your existing internal email server on the internal network can be addressed.	
Email domains: Enter the domains of email addresses of your organization, such as firm.ch, firm.com, firm.de.	

Required information to set up the SEPPmail appliance

* The SEPPmail appliance must be accessible from the Internet as a web server and therefore requires an externally accessible IP address. This is often the address of the firewall or reverse proxy / web application firewall. In simple installations, the IP address under which your Internet router is

© 2014 SEPPmail AG

accessible externally can be used.

You can find this information using the following steps:

1. Open a command prompt on a Windows PC, enter the command "nslookup" and press Enter.
2. Enter after the ">" character (Prompt) "set querytype=mx" and press Enter.
3. Enter the email domain of your organization (e.g. yourdomain.com) and press Enter.
4. You will receive one or more responses with the term "mail exchanger ="

Server name behind the term "mail exchanger" with the lowest MX preference number has the highest priority for name resolution.

© 2014 SEPPmail AG

3.4 Connecting SEPPmail appliance

In case you have purchased the VM version (Virtual Machine) of SEPPmail appliance, start your virtual appliance.

If you have the hardware version, connect the SEPPmail appliance, as follows:

1. Connect the Ethernet interface labeled »LAN1« or »eth0« from the SEPPmail appliance to the Ethernet port on your computer. Use a crossover RJ45 patch cable for the connection (also known as a crossover cable). Alternatively, you can use an Ethernet hub or Ethernet switch with a normal RJ45 patch cable.

2. Connect to the appliance to the power supply using the enclosed power cord.

3.5 Setting up Firewall / Router

Define on your firewall i.e. your Internet router, the following rules to ensure the secure email communication through SEPPmail

Port	Source	Target	Description	
TCP/22 (SSH)	Appliance	Internet	Makes it possible to perform updates to the appliance and includes support sessions for the user.	
TCP/22 (SSH)	Appliance	Appliance	Is required when operating with multiple appliances in the cluster compound.	**
TCP/25 (SMTP)	Email server	Appliance	Is needed to provide the internal email server ability to send outgoing emails to the appliance to be encrypted or signed there.	
TCP/25 (SMTP)	Internet	Appliance	Enables email traffic between the Internet and appliance.	
TCP/25 (SMTP)	Appliance	Internet	Is required for the direct transfer of emails to the Internet.	
		Email server	Is required for sending emails to an internal mail server.	**
UDP/53 (DNS) TCP/53 (DNS)	Appliance	Name server (internal)	Enables name resolution when internal DNS servers are used.	**

© 2014 SEPPmail AG

Port	Source	Target	Description	
		Name server (external)	Enables name resolution, when using external DNS servers.	
		Internet	Enables name resolution if the setting »built-in DNS Resolver« is used.	
TCP/80*	Appliance	Internet	Will be needed for the Protection Pack (Virus, Spam and Phishing Protection) updates.	
TCP/443 (HTTPS)	Internet	Appliance	Sets the encrypted communication over SSL (HTTPS) to SEPPmail. This will be needed to use the GINA technology.	
UDP/6277*	Appliance	Internet	Will be needed for Protection Pack with DCC.	
UDP/24441*	Appliance	Internet	Will be needed for Protection Pack with Pyzor.	
TCP/UDP/123* (NTP)	Appliance	Internet	Enables time synchronization.	
TCP/8080* (HTTP) and/or TCP/8443* (HTTPS)	Admin PC	Appliance	Sets the secure administrator access on the internal network. It is recommended, that only SSL encrypted connection (HTTPS) is allowed via port TCP/8443.	**
TCP/5061*	Appliance	Internet	Will be is used for the SMS transfer.	

Rules for ensuring the network communication of the SEPPmail appliance

* optional, depending on the configuration of the SEPPmail appliance
** In simple installations, no firewall between the SEPPmail appliance and the internal network is used. Rules marked with ** rules are then omitted.

© 2014 SEPPmail AG

3.6 Network settings and System Registration

The following describes, how you can integrate your SEPPmail appliance in your network and can check the network communication. These include the definition of the IP address(es) of your SEPPmail appliance, DNS settings, the default gateway setting, the entry of a host name and the specification of your internal domain.

At the end you can check, if the settings are correct by using the »Check Update« function of the appliance and register your system.

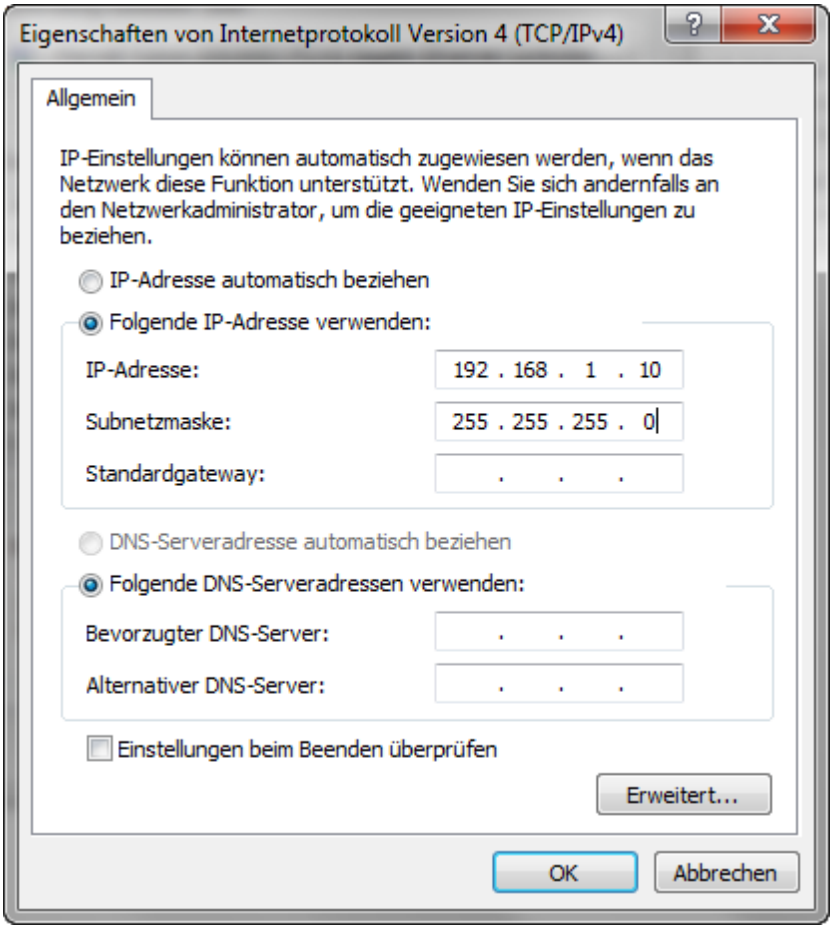
3.6.1 Setting up installation PC

For the initial configuration of the network parameters of your SEPPmail appliance, your computer must be connected on the same network, that the appliance itself. If this is not already set up in the IP address range of 192.168.1.xxx/24, change the IP address of your computer to an IP address between 192.168.1.1/24 - 192.168.1.254/24, network mask 255.255.255.0.

Note:

Do not use the address 192.168.1.60, which is reserved for the SEPPmail appliance. This is the default IP address upon delivery.

An example of appropriate network settings are shown in the following figure.


Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 1 . 10
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway:
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server:
Alternativer DNS-Server:
Einstellungen beim Beenden überprüfen
Erweitert...
OK
Abbrechen

© 2014 SEPPmail AG

3.6.2 Logging in as Administrator

All administrative options for SEPPmail appliance are available through a web browser-based configuration interface. On delivery, you can access the configuration interface at the following address:

LAN1 - https://192.168.1.60:8443
LAN2 - https://192.168.2.60:8443

The default user name is : admin
The default password is : admin

Note:

You will receive at this stage the message »No valid license found - Please obtain a valid license«, because the SEPPmail appliance is supplied with a temporary license. Follow the further instructions in this chapter for basic set up and to register your system. This will give you a permanent license and you can make full use of the SEPPmail appliance.

When you call the configuration interface in your web browser, you receive an error message indicating that the SSL certificate of the website is void. Select the option to call this page anyway.

Note:

The message only appears initially to get a valid SSL certificate installed (see »SSL« menu item 103).

3.6.3 Network settings of the SEPPmail appliance

To configure the network parameters of your SEPPmail appliance, click in the configuration interface on the »System« menu item.

»IP Addresses« section

Parameter	Description
Interface 1 - IP address	IP address of the network interface for the »LAN1« i.e. »eth0«
Netmask	Network mask for the IP address of the interface

Note:

The definition of the netmask is determined by the Classless Inter-Domain Routing (CIDR) notation.

- The netmask 255.255.255.255 corresponds "/32" (single IP addresses)
- The network mask 255.255.255.0 corresponds "/24" (Class C network)
- The netmask 255.255.0.0 corresponds to "/16" (class-B network)
- The netmask 255.0.0.0 corresponds to "/8" (class-A network)

© 2014 SEPPmail AG

»DNS« section

Parameter	Description
Primary	IP address of the DNS server Note: Please make sure that the DNS entries are correct. Internet domain names should be resolvable by the registered DNS server. Incorrect entries can lead to a very slow response of the configuration interface, such that the loading of menu items can take several minutes. Alternatively, you can use the setting »Use built-in DNS Resolver«. If you use this option, make sure, that you set up your firewall or router so, that the SEPPmail appliance can perform DNS resolution via the root DNS server on the Internet (see chapter Setting up firewall/ router 17).
Alternate 1	IP address of another DNS server, if the primary DNS server is not responding

3.6.4 Assigning host and domain names

To configure the host name and the domain name of your SEPPmail appliance, click in the configuration interface on the »System« menu item. Enter the appropriate values in the »Hostname« and »Domain« fields.

The host name can can freely chosen, securemailgateway, for example. The domain name is the DNS domain, within which the appliance is located (e.g. yourfirm.local or yourdomain.com). These settings are set from the internal point of view, so they do not need to correspond to the data, as they would have to comply for validity from the Internet.

3.6.5 Checking the network configuration

Perform the following steps to ensure, that the SEPPmail appliance works with your network settings:

1. Click in the configuration interface on the »Administration« menu item.
2. Click the »Check for Update« button.

If you receive one of the following two messages, the network configuration was successful:

- »You already have the latest version installed«
- »There is a new version available: installed version is OldVersionNumber, latest version is NewVersionNumber«

Otherwise, the message »ERROR: unable to connect to update server. Make sure that the

© 2014 SEPPmail AG

device can make connections to the Internet on port 22«. If this message appears, check again to make sure your network settings are correct and if your firewall i.e. your router allows the connection of your appliance to the Internet via port TCP/22 (SSH) (see chapter Setting up firewall/ router) 17.

3.6.6 Bringing the system to the latest version

Click on the web administration portal on the »Administration« menu item and then click the »Check for Update« button. If an update is available, click in addition on the»Fetch Update« button. This can be time consuming, if the delivered system still contains an older firmware and must therefore perform multiple updates.

Repeat this step until no more updates appear. The system optimizes this process, so that an update does not need to be performed for each intermediate version, but only for those that change the data structure.

It may be in certain circumstances take that you will not get any feedback for a long time. If this is the case, refresh the view by clicking on the »System Administration« link above the buttons. As long as you have not logged out, the update is not completed yet.

The SEPPmail appliance must reboot for each update. Perform this step, if necessary by yourself, in case the system gives no response for a long time, and you may not even see the login screen displayed. You can trigger the reboot by clicking within the »Administration« menu on the » Reboot« button, and then confirm the security code shown. Check after reboot again each time whether further updates are available.

If you see the message »You already have the latest version installed«, your SEPPmail appliance is up to date. Should there be more updates available in the future, this will be automatically indicated in each case after a reboot.

3.6.7 Registering the system

Register your system to get a permanent license. Click the web administration portal on the »Administration« menu item and then click the »Register this device...« button.

You will see a registration window. Fill in the fields in the registration window with your details. Enter into the upper half your customer information and in the lower half the data of your source of supply. Complete the entries by clicking the »Send« button.

If the »Registration successful« message appears, you have successfully completed the registration process.

© 2014 SEPPmail AG

3.7 Important safety measures

The following safety measures are described in the next sections :

Changing the administrator password 23
Setting the HTTPS protocol for secure access to the appliance 23
Creating a backup user to regularly backup the appliance 23

3.7.1 Changing Administrator Password

Please make sure that the »admin« user password is changed and is set to a corresponding complex value. Sign up as »admin« user on to the system and click on the »Users« menu. Select there the »admin« user. You can change the password and make other settings, that affect the »admin« user.

3.7.2 Setting the HTTPS protocol for secure access to the system

Under the »System« menu item, you will find the »Advanced View« button. Click this to view other configuration options. In the »GUI Protocol« and »GINA https Protocol« sections, you can set whether corresponding requests should be made to the appliance via HTTP or HTTPS.

We recommend, for security reasons, disabling the the HTTP option and also allow the configuration interface »GUI Protocol« as well as »GINA https Protocol« only for HTTPS.

3.7.3 Creating backup user

To back up the configuration of the SEPPmail appliance regularly, set up a backup user for this purpose. The backup of the appliance is encrypted and sent daily to the email addresses of all backup users.

To create a backup user, click on the »Users« menu item and then click the »Create new user account...« button. Fill in the fields »User ID«, »Full Name«, »E-Mail« and »Password«. Make sure that the email address is a valid address. Click the »Groups« menu. In the »backup (Backup Operator)« pane, click the »Edit...« button. Add the required users to the list of group members.

Setting backup password

To be able to proceed to the backup of the appliance, also a backup password must be set. Backups of the appliance are encrypted using this password. During a restore of the appliance by importing a backup file, this password must be entered.

To set the password, click on the »Administration« menu item and then click the »Change Password« button in the »Backup« section.

© 2014 SEPPmail AG

3.8 Next steps

You now have created the basis for secure email traffic through the SEPPmail appliance.

Perform the following 5 steps to achieve a minimal configuration for secure email exchange:

1. Set the date and time and setting up NTP synchronization 50
2. Set up for managing email domains 58
3. Email relay settings 61
4. Create self SSL certificate 103 (for the test operation)
5. Request SSL certificate from a public CA 105 (for productive operation)

The following two points are described hereafter.

Do this only after the preceding steps are through, in order to not to interfere with the email traffic.

1. Convert email data flow 24
2. Use email clients 26

3.8.1 Converting email data flow

To enable secure email traffic with the SEPPmail appliance, you must make the following changes to your existing email server:

1. Authorize SEPPmail appliance for email sending with email relay setting
2. Define SEPPmailappliance as a smart host

Make sure that the email traffic using SEPPmail appliance to external is possible by setting up your firewall or router as described previously (see chapter Setting up Firewall / Router 17).

As soon as you integrate SEPPmail appliance into your email data flow, you also need to replace the IP address of your existing email server in your firewall rules with the IP address of the appliance.

As soon as you integrate the SEPPmail appliance in your email data flow, you must ensure, that the emails from external no longer are transported to the email server, but to SEPPmail. This can be set up in the firewall or an upstream SPAM filter, depending on your network infrastructure.

SEPPmail sends by default emails directly to the Internet. If the email traffic is to take place through an SMTP gateway (relay), set up your appliance correspondingly (see Controlling Outbound Mail Traffic 58).

Authorization for email dispatch

To enable email delivery from your SEPPmail appliance to your existing email server, you must authorize the appliance for it. This setting is usually defined as an SMTP email relaying. Apply for this purpose the internal IP address or internal host name of the SEPPmail appliance on your email server in the list of authorized email relay systems.

© 2014 SEPPmail AG

Definition of SEPPmail appliance as a smart host

The SEPPmail appliance is after the integration in the role of an SMTP gateway in your email environment. Your email server will then no longer forward emails directly to the external, but (new) to the SEPPmail appliance.

To make this change, you need to define the internal host name or the internal IP address of your SEPPmail appliance on your existing email server as Smarthost.

ATTENTION

With this adaptation, you change the email communication by integrating the SEPPmail appliance in the mail data flow. All emails will be, after the change, sent to the SEPPmail appliance.

Perform this change only, when all other configuration steps of the SEPPmail appliance are complete. Otherwise it may lead to an impairment of the email traffic.

© 2014 SEPPmail AG

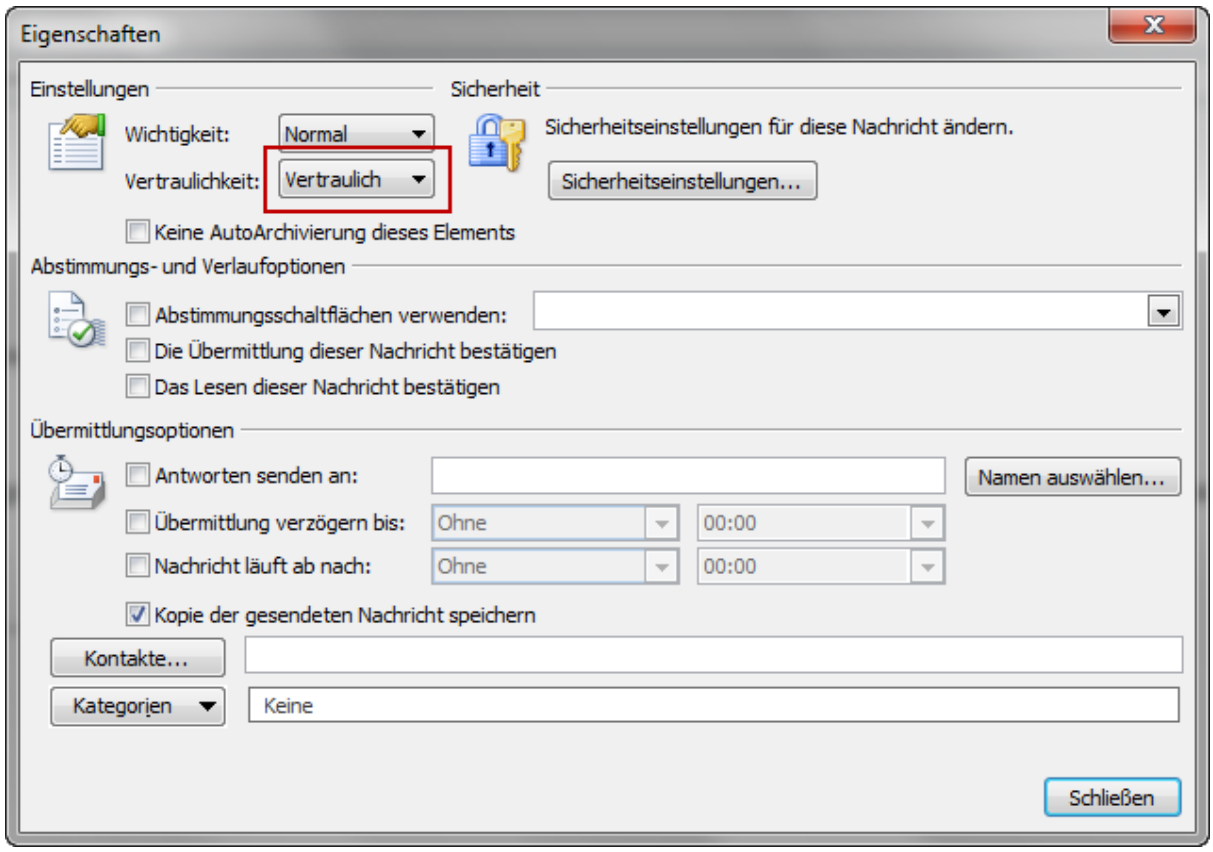
3.8.2 Using email clients

The use of standardized procedures and the central processing by the SEPPmail appliance ensures the independence of the local email client. No adjustments to the email clients are therefore required.

The users have, within their email clients, the following control options for sending encrypted emails:

- Select in MS Outlook the message option »Confidential«.
- Type in alternatively the subject line of the [secure] tag. This is the defined default term, which triggers an encrypted email sending.

In addition to the [secure] tag, there are other terms available, for example for signing emails. You can view and adjust, if necessary, the terms in the configuration interface in the »Mail Processing« menu in the »Ruleset Generator« section. For more details, see chapter Managing Ruleset 89.



Message option »Confidential« in Outlook

© 2014 SEPPmail AG

4 Microsoft Outlook Add-In

4.1 Introduction

The SEPPmail add-in for Microsoft Outlook can be installed on PC systems with Microsoft Outlook. The installation can be done with user dialog or in silent mode without user interaction. Depending on the installation, different settings (parameters) are available to affect the functionality of the add-ins.

The add-in itself provides various from email window definable buttons (for writing an email) for use. Depending on the settings chosen during installation, there is a different number of buttons, with different default settings (pressed / not pressed).

The states of the main buttons in the subsequently sent emails, will be integrated in the form of control information in the header of the email and evaluated by the central SEPPmail system. A button (optional) displays a help page in the default web browser. A setting (optional) can be applied in order to display a warning, when sending unencrypted and unsigned emails.

The usage is multilingual and adapts to the language of the Microsoft Outlook interface. If this is not available, English is the default language for the add-in.

The following technical details for the system requirements, installation, the procedures in the registry and for sending emails are described.

4.2 System requirements

The SEPPmail add-in for Microsoft Outlook can be installed under different operating systems and Microsoft Outlook versions:

Microsoft Windows operating systems:

- Windows XP
- Windows Vista
- Windows 7 (32 bit and 64 bit)
- Windows Terminal Server

Microsoft Outlook versions:

- Outlook 2000
- Outlook XP
- Outlook 2003
- Outlook 2007
- Outlook 2010 (32 bit)
- Outlook 2010 (64 bit)

.NET Framework:

The .NET Framework requires the version 3.5 SP1 or newer available. If it is missing, the installation routine tries to obtain this component automatically from the Internet and install it.

© 2014 SEPPmail AG

4.3 Download

You can download the current version of the SEPPmail add-in for Microsoft Outlook at the following Web page:

http://dl.seppmail.ch

4.4 Installation

The installation consists of two files:

Setup.exe

- It is mandatory, when running on Windows Vista and Windows 7, while the UAC is switched on, to be able to select "As administrator" by right-clicking.
- Verifies before running the .msi file, whether the conditions for the installation (e.g. NET Framework) are satisfied.

SecureMailAddInSetup 1.2.6.msi

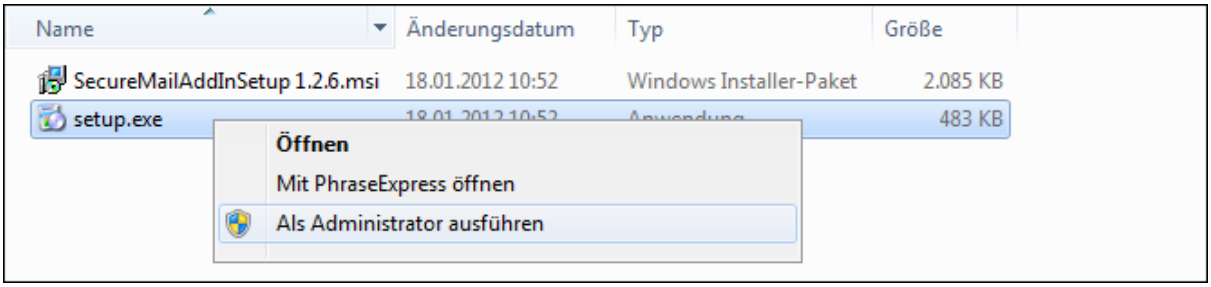
- Performs the actual installation.
- Can also be started directly, when corresponding rights are available (e.g. inactive UAC and administrator rights).
- Can also be used for automated software deployment.

© 2014 SEPPmail AG

4.4.1 Installation with a user interface

Example: Windows 7 (64 bit)

1. Right-click the »setup.exe« file and select »Run as administrator«.



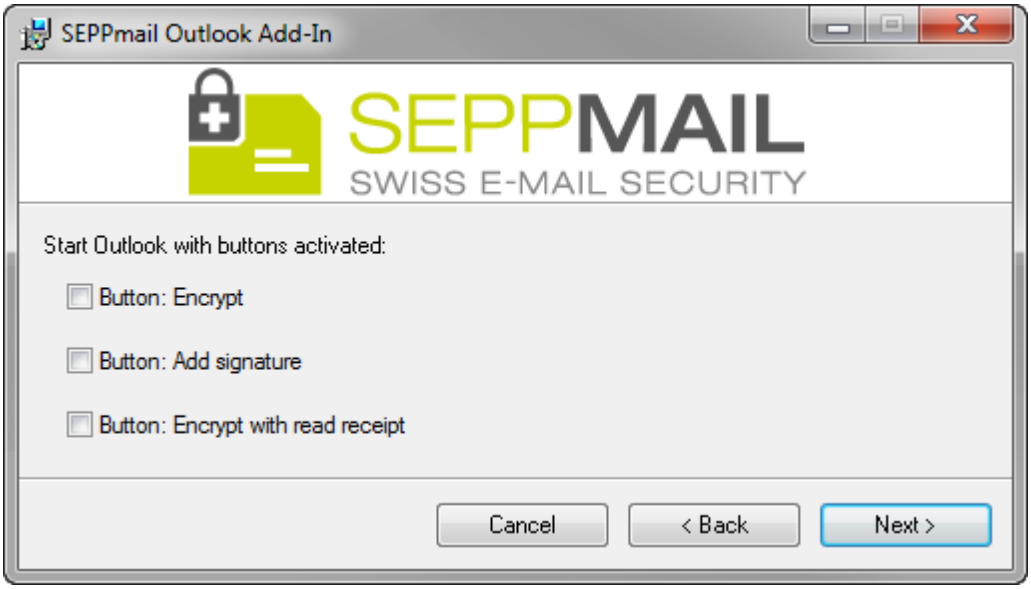
Installation - Outlook Add-In

2. Answer the Windows confirmation prompt with »Yes« to start the installation.
3. After this, the following screens appears offering the user the options:
   a. the buttons to be displayed
   b. turning on and off a warning, when sending unencrypted and unsigned emails
   c. the default buttons states, when opening an email window

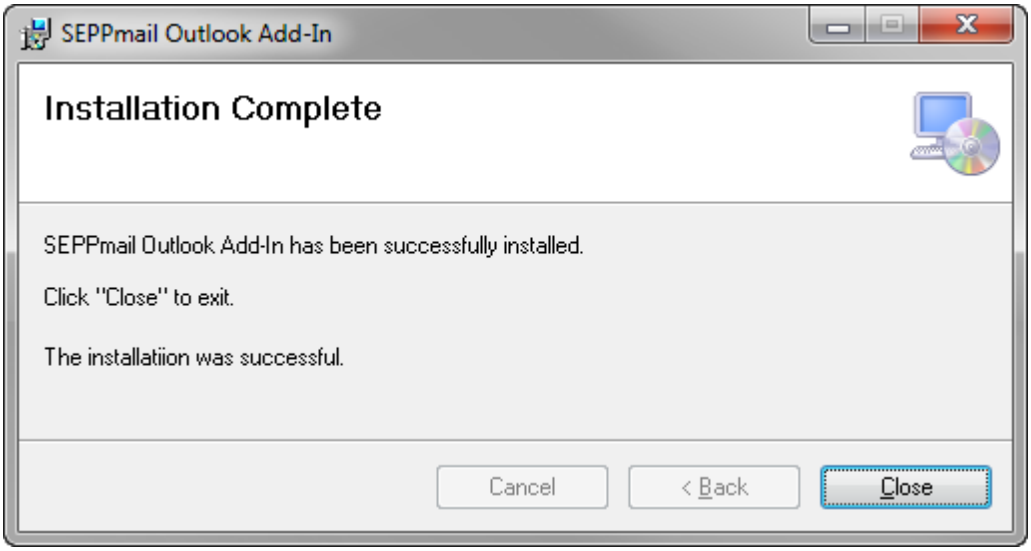
SEPPmail Outlook Add-In
SEPPMAIL
SWISS E-MAIL SECURITY
Please select the options that should be available within Outlook.
Button: Encrypt
Button: Add signature
Button: Encrypt with read receipt
Warning Message for unencrypted or unsigned outgoing e-mails.
Cancel
< Back
Next >

Installation - Outlook Add-In - hidden buttons - warning

© 2014 SEPPmail AG



Installation - Outlook Add-In - active buttons



Installation successfully completed - Outlook Add-In

© 2014 SEPPmail AG

4.4.2 Installation without a user interface

The installation can alternatively be started from the command prompt using various parameters.

Note:

The command prompt must be started as administrator!

Example: (call as separate command lines)

```
msiexec /q /i "SecureMailAddInSetup 1.2.6.msi" SMWarning=false
SMEncrypt=true SMSign=true SMWebmail=true SMHelp=true
SMEncryptSelected=false SMSignSelected=false SMWebmailSelected=false
/li .\log.txt
```

Msiexec parameter:

Parameter	Description
/q	Installation without a user interface
/i	Installation of an msi package
/li	**.\log.txt log.txt** generates basic information in the current directory

MSI parameter: (underlined in each case of the default value)

Parameter	Description
SMWarning (true/false)	Warning for unencrypted emails **switch on/off**
SMEncrypt (true/false)	Encrypt **switch on/off**
SMSign (true/false)	Sign **switch on/off**
SMWebmail (true/false)	Encrypt with read receipt **switch on/off**
SMHelp (true/false)	Help **switch on/off**
SMEncryptSelected (true/false)	Encrypt **Default: active/inactive**
SMSignSelected (true/false)	Sign **Default: active/inactive**
SMWebmailSelected (true/false)	Encrypt with read receipt **Default: active/inactive**

© 2014 SEPPmail AG

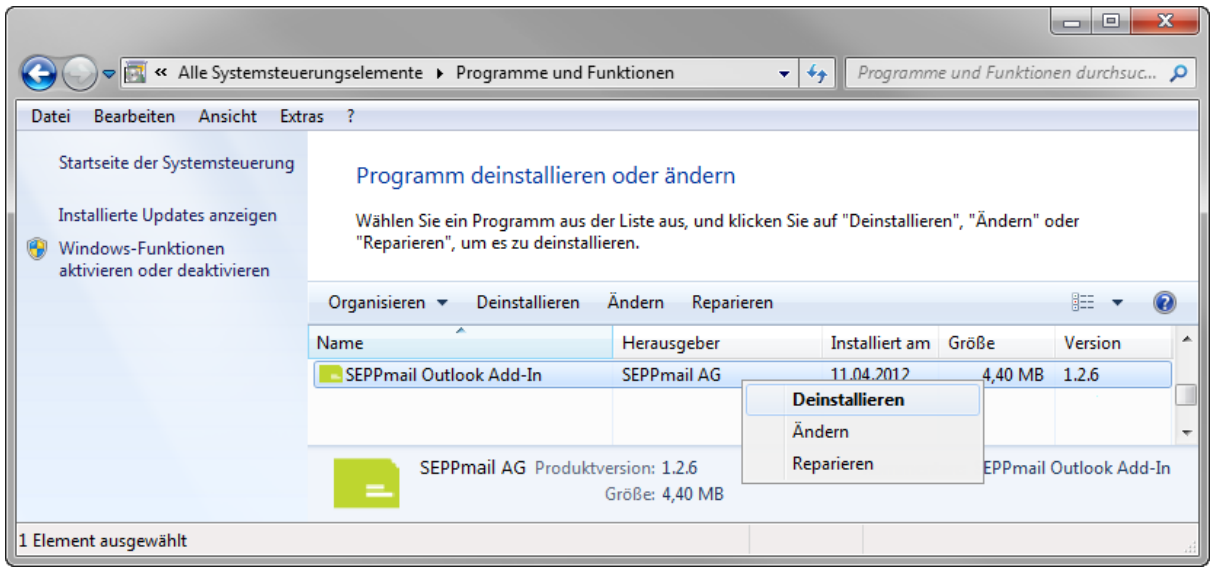
Parameter	Description
Tooltips (true/false)	Tool tips for buttons **switch on/off**
LMonly (true/false)	Save registry values only in HKEY_LOCAL_MACHINE **switch on/off**

4.5 Uninstallation of Microsoft Outlook Add-In

Uninstallation of SEPPmail Add-In for Microsoft Outlook is done via the »Control Panel« in » Programs and Features« menu.

Example: Windows 7 (64 bit)

1. Right click on the entry »SEPPmail Outlook Add-In -> Uninstall«.

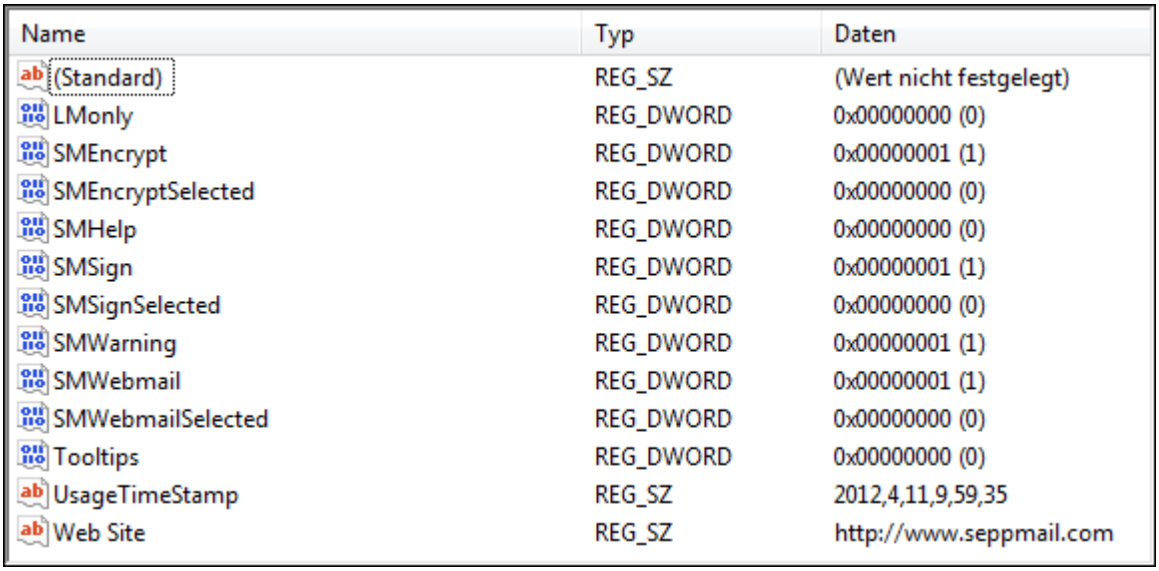

« Alle Systemsteuerungselemente ▸ Programme und Funktionen
Programme und Funktionen durchsuc...
Datei Bearbeiten Ansicht Extras ?
Startseite der Systemsteuerung
Installierte Updates anzeigen
Windows-Funktionen aktivieren oder deaktivieren
Programm deinstallieren oder ändern
Wählen Sie ein Programm aus der Liste aus, und klicken Sie auf "Deinstallieren", "Ändern" oder "Reparieren", um es zu deinstallieren.
Organisieren Deinstallieren Ändern Reparieren
Name Herausgeber Installiert am Größe Version
SEPPmail Outlook Add-In SEPPmail AG 11.04.2012 4,40 MB 1.2.6
Deinstallieren
Ändern
Reparieren
SEPPmail AG Produktversion: 1.2.6
Größe: 4,40 MB
EPPmail Outlook Add-In
1 Element ausgewählt
Uninstallation - Outlook Add-In

© 2014 SEPPmail AG

4.6 Registry entries of the Microsoft Outlook Add-In

4.6.1 HKEY_LOCAL_MACHINE

During the installation, only values in the registry branch »HKEY_LOCAL_MACHINE« are written, since the installation of the add-ins for all users of a PC/terminal server follows. The following values are written by default:



Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
LMonly	REG_DWORD	0x00000000 (0)
SMEncrypt	REG_DWORD	0x00000001 (1)
SMEncryptSelected	REG_DWORD	0x00000000 (0)
SMHelp	REG_DWORD	0x00000000 (0)
SMSign	REG_DWORD	0x00000001 (1)
SMSignSelected	REG_DWORD	0x00000000 (0)
SMWarning	REG_DWORD	0x00000001 (1)
SMWebmail	REG_DWORD	0x00000001 (1)
SMWebmailSelected	REG_DWORD	0x00000000 (0)
Tooltips	REG_DWORD	0x00000000 (0)
UsageTimeStamp	REG_SZ	2012,4,11,9,59,35
Web Site	REG_SZ	http://www.seppmail.com

Registry - HKEY_LOCAL_MACHINE

The path in the registry is:

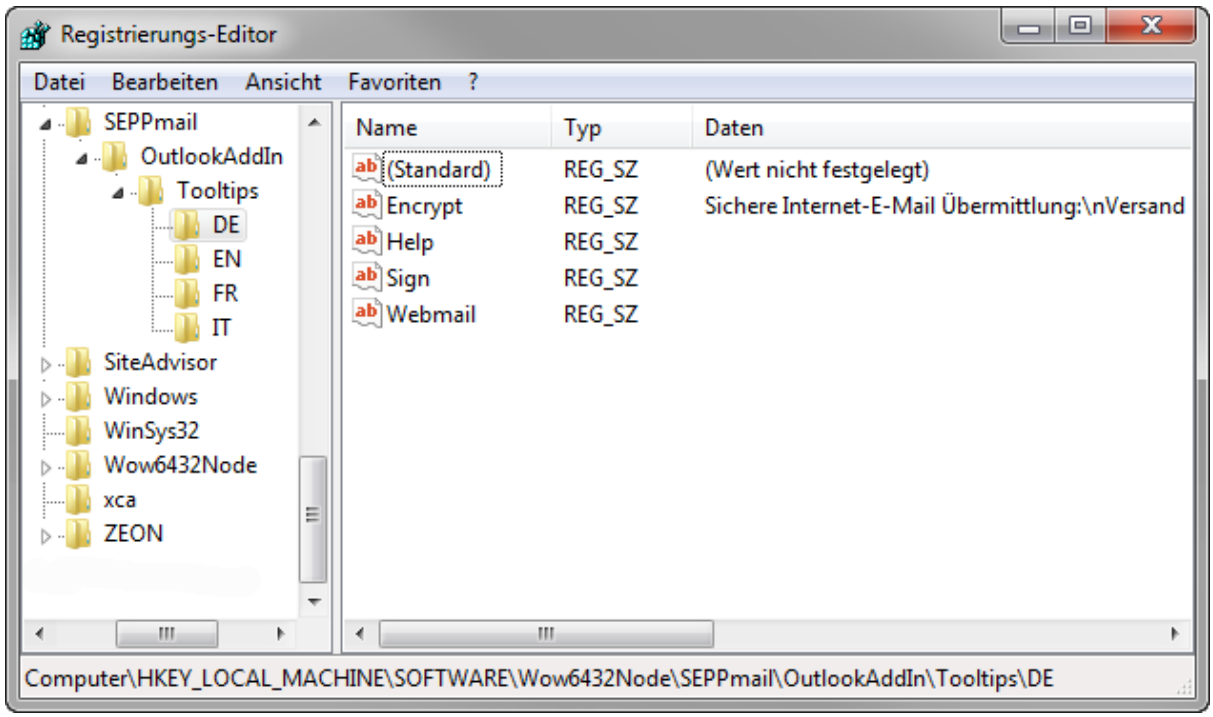
```
HKEY_LOCAL_MACHINE\SOFTWARE\SEPPmail\OutlookAddIn
```

On 64 bit systems (since the setup package runs in 32 bit mode), the following path is used:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SEPPmail\OutlookAddIn
```

In this registry key, a sub folder/key exists, which is named Tooltips. The tooltips for the buttons will be stored in folders for each language as follows:

© 2014 SEPPmail AG



Registry - Tooltips

© 2014 SEPPmail AG

4.6.2 HKEY_CURRENT_USER

If the option »LMOnly = false« is set in the registry branch »HKEY_LOCAL_MACHINE« (default value), it will be checked at the start of Microsoft Outlook, whether registry values for the add-in are already in the pane

```
HKEY_CURRENT_USER\Software\SEPPmail\OutlookAddIn
```

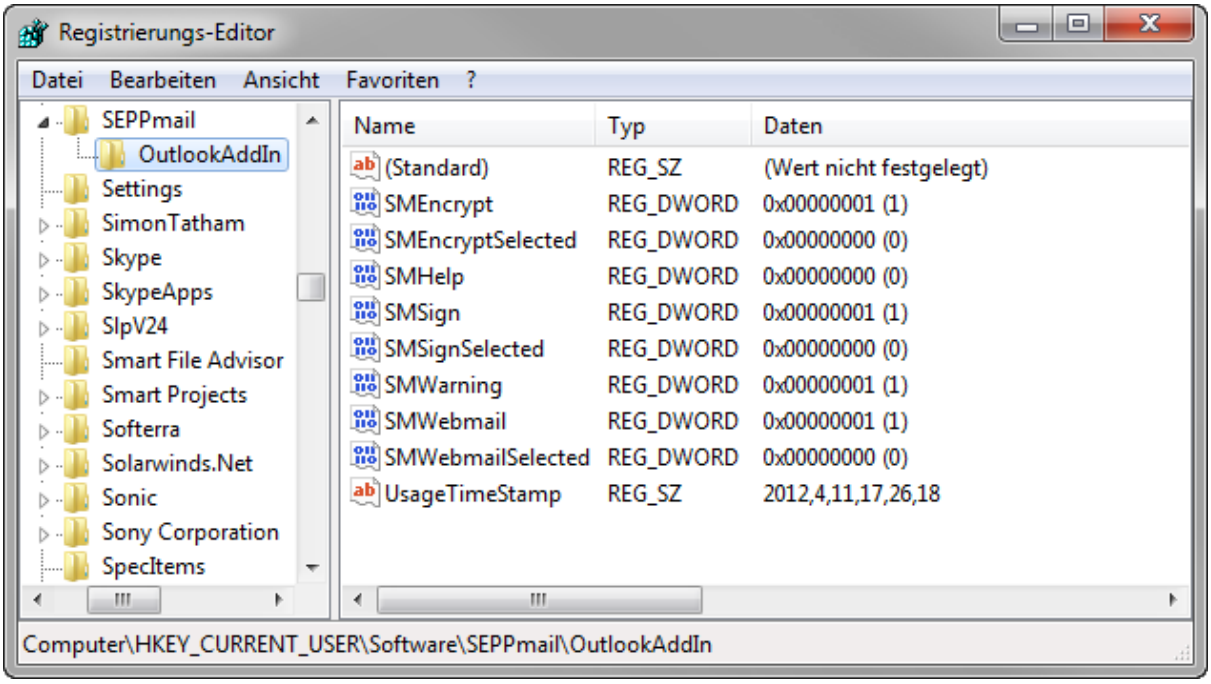
i.e.

```
HKEY_CURRENT_USER\Software\Wow6432Node\SEPPmail\OutlookAddIn
```

are available.

If yes, the time stamp (usage timestamp) is compared between the settings from » HKEY_LOCAL_MACHINE« with those of »HKEY_CURRENT_USER«.

If the settings from »HKEY_LOCAL_MACHINE« are newer (or no value in » HKEY_CURRENT_USER« exists), then the following settings are copied from » HKEY_LOCAL_MACHINE« to »HKEY_CURRENT_USER«:



Registry - HKEY_CURRENT_USER

The time stamp (Usage timestamp) in »HKEY_CURRENT_USER« is thereby assigned to the current time.

This makes it possible for the settings to be set on the buttons individually for the users, without causing the settings for other users to be impaired.

If the time stamp (usage time stamp) of »HKEY_CURRENT_USER« is newer than that of » HKEY_LOCAL_MACHINE«, then the values from »HKEY_CURRENT_USER« are always used by the add-in.

© 2014 SEPPmail AG

4.7 Sending emails

When sending emails, the following fields will be written in a separate header of the email, depending on the status of the buttons:

Parameter	Value
x-smenc	**yes/no**
x-smsign	**yes/no**
x-smwebmail	**yes/no**

© 2014 SEPPmail AG

5 SEPPmail - IronPort connection

Attention:

It is important to understand the current policy of the IronPort Systems before changes are made.

Suggested configuration

All incoming emails are received by IronPort and checked for spam and viruses. All emails certified as far will be forwarded to SEPPmail, where they are, if necessary, decrypted and sent back to IronPort. There, all the emails are (now decrypted), again virus and spam tested and passed to the internal groupware system, e.g. MS Exchange or Lotus Notes., passed

Alternatively, it is possible to recognize the encrypted and/or signed emails on the IronPort system and redirect only those to SEPPmail. All other emails will be forwarded directly to the internal groupware system.

The internal groupware system sends the outgoing emails to IronPort. This forwards outgoing email in every case further to SEPPmail. There, the ruleset will maintain, which emails are to be signed and encrypted. Subsequently, the outgoing emails are sent from the SEPPmail system back to the IronPort system, which as the only system, sends emails towards the Internet.

The »problem« with this configuration is that SEPPmail must stay in the relay list of IronPort Systems, as the SEPPmail system tries to send the outgoing emails towards the Internet. For all hosts in the relay list of IronPort always automatically applies the »Outgoing Mail Policy«. According to the current »Outgoing Policy«, no virus scan is taking place there, and therefore the SEPPmail connection as such provides no additional benefit.

There are two solutions to this:

1. You build the »Outgoing Mail Policy« on the IronPort system so, that they look similar to the »Incoming Policy«. But this is an »ugly« solution.

2. You configure a specific listener via which the SEPPmail delivers incoming emails. The SEPPmail must not be registered in the relay list in this listener. This listener can, for example, be bound to the existing IP address 192.168.1.11 on a specific port (e.g. 10025) or to another IP address in the IP network 192.168.1.0/24.

The redirection can be implemented in two ways:

1. by Content Filter
2. by Message Filter

The difference between Message Filter and Content Filter is that a Message Filter is always applied to the entire email. If an email has, for example, multiple recipients, then the action applies to all recipients. In a Content Filter you can split the email via different policy entries. That should not play any role in our case. Another difference is, that you can see in the message filter, whether an email is encrypted or signed, so that only this email can redirect to SEPPmail.

To make the solution simple and clearly structured, we recommend all outgoing emails to be forwarded to SEPPmail (not just emails to be encrypted or signed) and to work with a Content Filter.

© 2014 SEPPmail AG

Configuration

IronPort

- Existing Listener with SEPPmail in the Relay List
- New listener Incoming SEPPmail with SEPPmail not in the Relay list

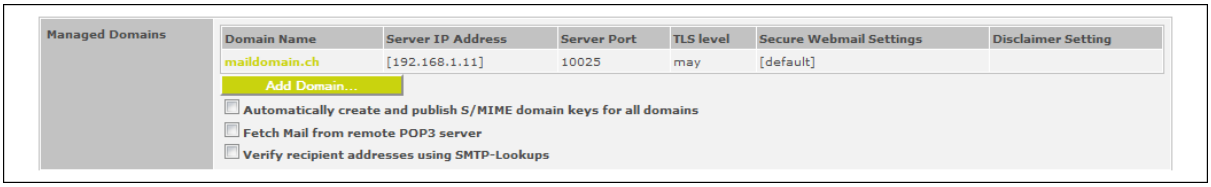
Incoming Contentfilter : IncomingSEPPmail

```
(usually not required: Receiving Listener = IncomingMail AND)

Remote IP IS NOT \[IP from SEPPmail 1\]
AND
Remote IP IS NOT \[IP from SEPPmail 2\]

(optional, if you only have one of your domains on SEPPmail
want to let operate: AND Envelope Recipient
ends with @securemailcustomer.ch )

Action: Send to Alternate Destination Host: \[Cluster IP of both SEPPmail\]
```

SEPPmail

The SEPPmail system is set up so that incoming emails are sent to the incoming SEPPmail listener.

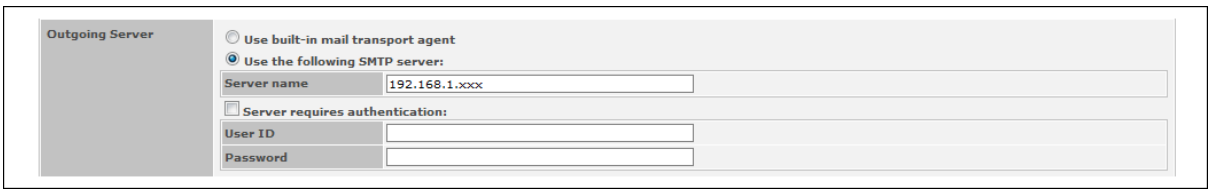
Mail menu system: see Managing Email Domains Setup 58



Managed Domains section

The problem here is that in the SEPPmail configuration, only a single IP address can be specified, to where the incoming emails are forwarded, but not both incoming IP addresses of your IronPort. For this reason, it is necessary to generate a (fictitious) DNS entry, which can be dissolved in both IP addresses of the IronPort. Enter this DNS name as »Server IP Address« of the email domain.

Outgoing email sent SEPPmail to the existing listener:
See Controlling Outgoing Email Traffic 58

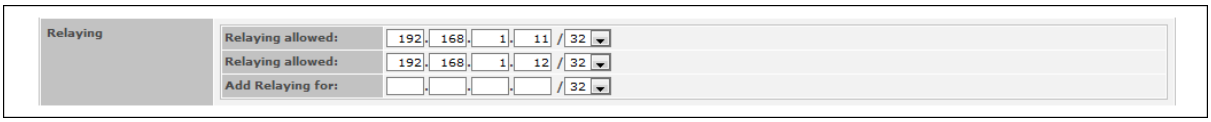


Outgoing Server section

© 2014 SEPPmail AG

The IP address of the listener shall be specified here, i.e. a host name as above, which will dissolve on both listeners.

For both IP addresses of IronPort system the SEPPmail system registers the relay permission. See Mail Relaying 61.



Relaying section

The configuration description for the SEPPmail IronPort connection was provided us by courtesy of:

AVANTEC AG
Badenerstrasse 281
CH-8003 Zürich
http://www.avantec.ch
info@avantec.ch

© 2014 SEPPmail AG

6 Reference of the menu items

6.1 Configuration Overview

The configuration user interface of the SEPPmail appliance is divided into the following groups:

The following table lists all groups with a brief description. The structure of this part of the manual is based on the structure of these groups.

Groups	Description
Login	Log in to the configuration interface, change the personal password for the configuration user interface
Home	Display administrative data such as system status, system and user license, current software version, statistical data on system utilization
System	Perform basic network settings, such as IP address, host name and domain name, routing, system date and time
Mail System	Setting up the SEPPmail mail system, email domains and email routing, mail relay server, access control, TLS, anti-spam, blacklists/whitelists
Mail Processing	Govern email processing, manage GINA domains, govern SMS password sending, disclaimer, email templates, virus scanning spam protection rules and thresholds, rulesets for email signing, manage/view/load encryption and decryption
SSL	SSL device certificate for setting up and securing the SEPPmail secure web mail web server
CA	Setting up your own certificate authority (CA), setting up connector for SwissSign CA, requesting and securing CA certificate
Administration	Register SEPPmail, install software updates, create backup and back securing, restart or shut down SEPPmail, reset SEPPmail to factory settings, import existing user or key, activate outgoing support connection
Cluster	Setting up a cluster composite systems with several SEPPmail systems
Logs	View and manage email log files
Statistics	Graphical display of the processed email traffic and system load
Users	SEPPmailCreate and manage user accounts
Groups	SEPPmailCreate and manage groups
GINA accounts	Managing automatically generated GINA accounts. GINA refers to the former secure web mail user interface.

© 2014 SEPPmail AG

Groups	Description
PGP public keys	Import and manage PGP public keys of communication partners
X.509 Certificates	Importing and managing public S/MIME X.50 certificates of communication partners
X.509 Root Certificates	Importing and managing S/MIME X.509 CA root certificates
Domain keys	Importing, synchronizing and managing PGP and S/MIME domain keys
Customers	Activate and set up a multi-customer configuration (multi-tenancy). Here can, for example, email domains, user accounts or GINA user accounts be dedicated to assign a previously defined customer.

Reference of the menu items in the SEPPmail configuration user interface

6.2 "Login" menu item

»Login« menu

Select the »Login« menu item, to log out of the SEPPmail configuration user interface or to change the appropriate user's password for the SEPPmail configuration user interface. The following table describes each parameter.

Parameter	Description
Login	User ID, Password To log in to the configuration user interface, select the »Log in« button.
Log out	To logout from the configuration user interface, select the »Log out« button.
Change Password	New Password You can change the password for the logged in user in this field. If you enter the new password, a point will be displayed for each character as placeholder. To avoid typing errors, it is necessary to enter the new password twice. To save the new password, select the »Change Password« button.

© 2014 SEPPmail AG

6.3 "Home" menu item

»Home« menu

»System Status« section

Parameter	Description
System Status	The current SEPPmail system status.

»License« section

Parameter	Description
License type	Information about the system and user license is displayed here.
License ID	License number for the SEPPmail system.
License Holder	Owner of the SEPPmail license.
Issue date	Date of issue of the license.
Comment	Additional information on the license.
Encryption/Signature Licenses	Number of user licenses purchased. The number of previously used user licenses is displayed in brackets.
Large File Management (LFM) Licenses	Number of user licenses purchased for the »Large File Management« function. The number of previously used user licenses is displayed in brackets.
Device License	Duration of the installed system license.
Software Care Pack	Displaying the expiration date of the license for software updates.
Device Care Pack	Displaying the expiration date of the Device Care Packs.
Protection Pack (Anti-spam / Anti-virus)	Displaying the expiration date of the license for anti-virus and anti-spam.
Internal Mail Encryption	License for internal encryption (Active / Inactive).
Self-Service password management	License for self-service password management (Active / Inactive).

© 2014 SEPPmail AG

»System« section

Parameter	Description
Device ID	Device license number
Appliance Type	Type of the current appliance, such as. SEPPmail 3000 (VMware Virtual Appliance).
Firmware Version	Currently installed software version on the system.
Uptime	Runtime of the system after the last reboot.

»Anti-Virus« section

Parameter	Description
Active / Inactive	Status of the optional virus scanner. This feature is only available, if you have purchased the paid Optional Software Protection Pack (anti-spam / anti-virus).

»Mail statistics« section

Parameter	Description
Mails Processed	Number of all completed transmitted emails (received, sent) by the system.
Mails Processed (S/MIME)	Total number of all emails (decrypted, encrypted) processed via S/MIME.
Mails Processed (openPGP)	Total number of all emails (decrypted, encrypted) processed via openPGP.
Mails Processed (DOMAIN)	Total number of all emails (decrypted, encrypted) processed via domain encryption.
GINA Mails	Total number of all secure web mails sent via the GINA subsystem.
Mails currently in queue	Number of all emails in the queue.

»Disk statistics« section

Parameter	Description
Database, Mail queue, Log, temp, LFM store	Displays the utilization of individual volumes of the hard drive used in the system separated by areas.

© 2014 SEPPmail AG

6.4 "System" menu item

Select the »System« menu, to make the basic network settings.

Following procedures are described in the chapters hereafter:

Overview 44
Sending mail logs to centralized syslog server 50
Setting date and time 50
Enabling SNMP 51

6.4.1 Overview of "System" menu item

»System« menu

The »System« menu can be viewed in two in two views. The essential basic settings can be viewed in the »Normal View«. This view is the default view, when accessing this menu. A complete overview of all settings can be seen in the »Advanced View«.

Advanced View

By pressing the »Advanced View« button, you can expand the list of available parameters. To summarize the expanded display of the »System« menu item again, press the »Normal View« button again in the expanded representation.

This menu shows the main parameters of the LAN connection of the SEPPmail system to be established. The data entered here also serve as the basic setting for many other settings of your SEPPmail systems.

»Comment« section

Parameter	Description
System Description	Enter a description that identifies the SEPPmail system. This parameter is, for example, used as the subject in the automatic data backup, otherwise used only for description.

»IP Addresses« section

Parameter	Description
Interface 1	Enter the IP address with subnet mask and the media type of the physical network interface »LAN1« i.e. »eth0«. By default, you can leave the media type to a value of »autoselect«. One interface configuration is displayed for any physically existing network interface. The here displayed interface number corresponds to the following network interfaces: Interface 1 - »LAN1« i.e. »eth0«

© 2014 SEPPmail AG

Parameter	Description
Interface 2	Enter the IP address with subnet mask and the media type of the physical network interface »LAN2« i.e. »eth1«. By default, you can leave the media type to the value »autoselect«. One interface configuration is displayed for any physically existing network interface. The here displayed interface number corresponds to the following network interfaces: Interface 2 - »LAN2« i.e. »eth1«
Custom hosts file entries:	To perform a local DNS name resolution, you can enter a combination of IP addresses and host names in this field. Format: 10.0.0.1 host.domain.tld

»IP ALIAS Addresses« section

Parameter	Description
IP Alias 0 - 3	1. Additional alias IP address of the interface 2. Network mask of the additional alias IP address 3. VHID (Virtual Host Identification) of the interface 4. Interface - Interface to which the additional alias IP address will be bound 5. Priority - priority of the interface in the cluster Additional information about the configuration options can be found in the description of the »Cluster« menu

»Name« section

Parameter	Description
Host name	Enter the host name of the SEPPmail system. E.g. securemail
Domain	Enter here the domain of SEPPmail system. E.g. seppmail.ch Note: The name of the system consists of the host name and the domain. E.g. securemail.seppmail.ch

»DNS« section

© 2014 SEPPmail AG

Parameter		Description
Use built-in DNS Resolver		With this parameter, the system will attempt DNS name resolution always using the DNS root name servers on the Internet. If you select this parameter, the resolution of DNS names can eventually take a long time and the response of SEPPmail system may be delayed thereby.
Use the following DNS Servers		DNS requests for addresses, for which SEPPmail is not self competent, are forwarded to higher-level DNS name server. For this, SEPPmail should pass on the DNS request to an internal DNS server on your own network or the DNS server of your Internet provider, which you can specify here.
	Primary	Enter here the first DNS name server, to which SEPPmail forwards DNS requests.
	Alternate 1	If the primary DNS name server is not available, or does not answer, you can arrange an alternate DNS name server to specify, where the DNS requests are to be forwarded.
	Alternate 2	If the primary and first alternate DNS name server are not available, or do not respond, you can specify here a further alternative DNS name server, to which DNS requests are then to be forwarded. Make sure that, if specified, the DNS name server is available, otherwise the function of SEPPmail may be impaired.
	Search Domain(s)	Enter a search list of domain names, that are queried when a DNS request is done sequentially.
local zone		»Domain name«: enter a pseudo domain name, for which you want to perform the local resolution in the IP address of the local email server (MX record), e.g. pseudo.local. host : hostname, e.g. mail mx : preference, e.g. 10 ip : IP address of the email server, e.g. 10.0.0.1 The server responsible for the domain pseudo.local email is now dissolved in mail.pseudo.local with the IP address 10.0.0.1 and the preference 10. Local zones can be used, if you cannot perform your own local DNS server for the resolution of the MX records for a domain and several alternate email servers for a domain are required as a failover.

»Routing« section

Parameter	Description
Default Gateway	Enter the IP address of the default router in your network segment. All data packets, which cannot be delivered directly

© 2014 SEPPmail AG

Parameter	Description
	on the local network segment are forwarded to these IP routers.
Static Routes	Besides the use of a default router, you can also specify static IP routes in the SEPPmail system. These IP routes have priority over the use of the default router.

»GUI Protocol« section

Parameter	Description
HTTP Port	Enable this parameter to allow unencrypted access via HTTP protocol to the configuration interface. Do this by specifying a corresponding TCP/port. This option is enabled by default, and uses port TCP/8080 to access the SEPPmail configuration interface.
HTTPS Port (default)	Enable this parameter to enable the encrypted HTTPS protocol access via the configuration interface. Do this by specifying a corresponding TCP/port. This option is enabled by default, and it uses the port TCP/8443 to access the SEPPmail configuration interface. Note: If the configuration interface via HTTPS stops responding due to an error, a fallback is automatically activated, which makes it possible to access the configuration interface via HTTP on port TCP/8080. This works even, when the use of HTTP has been disabled to access the configuration interface.

»GINA https Protocol« section

Parameter	Description
HTTP Port	Enable this parameter to allow unencrypted access via HTTP protocol to the Webmail interface of the SEPPmail system. Do this by specifying a corresponding TCP/port. The HTTP default port is TCP/80. Note: Do not use the HTTP protocol for access to the webmail interface from the Internet, or from another untrusted network. That allows thereby the logging of browser connections to the web mail interface of the SEPPmail.

© 2014 SEPPmail AG

Parameter	Description
HTTPS Port (default)	Enable this parameter to enable the encrypted access via HTTPS protocol to the webmail interface of the SEPPmail systems. Do this by specifying a corresponding TCP/port. The HTTPS default port is TCP/443.
Enable local https proxy, redirect unknown requests to http://	Reverse Proxy - enable this parameter to activate access to the webmail subsystem, no longer directly, but via the local SEPPmail Reverse-Proxy. You can also use the SEPPmail Reverse-Proxy for access to an internal OWA server (Outlook Web Access). On the OWA interface of the internal MS Exchange Server, must HTTP be enabled. The reverse proxy does direct all not for SEPPmail specific requests via HTTP further to the internal, e.g. a special landing page on the company website or to an OWA server. Likewise, also ActiveSync connections to the internal MS Exchange server are forwarded via the reverse proxy.

»Console Login« section

Parameter	Description
Disable console root login	Enable this parameter, to lock the console access to the SEPPmail system. Note: Please be aware, that when you activate this parameter, an intentional drop-in access to the system is no longer possible in case of failure.
Enable PIX workaround	Enable this parameter, if you are using a Cisco PIX firewall and the access to the system takes place via SSH through this firewall. Enabling this setting requires a restart.

»Syslog Settings« section

Parameter	Description
Forward maillog to syslog server	Host name or IP address of a syslog server on the LAN. The SEPPmail system logging is also sent to the specified syslog server. UDP/514 is used as the destination port.

»Proxy Settings« section

Parameter	Description
Proxy Server	Host name or IP address of the proxy server

© 2014 SEPPmail AG

Parameter	Description
Proxy Port	Destination port of the proxy server, e.g. destination port 8080 or 8081
Proxy User	Username for logging in to the proxy server
Proxy Password	Password for logging in to the proxy server
Use direct connection on port 22 outgoing (preferred)	Enable this option, if an SSH connection is possible directly without going through a proxy server on the Internet. An SSH connection uses the TCP protocol with destination port 22 (TCP/22).
Connect through SOCKS 4 proxy	Enable this option to tunnel SSH connections by a generic SOCKS proxy. This option can be used, when the direct access to the Internet is regulated via SSH, for that SEPPmail system, however, the connection through a SOCKS proxy (Version 4) to the Internet is possible.
Connect through SOCKS 5 proxy	Enable this option to tunnel SSH connections by a generic SOCKS proxy. This option can be used, when the direct access to the Internet is regulated via SSH, for that SEPPmail system, however, the connection through a SOCKS proxy (Version 5) to the Internet is possible.
Connect through HTTP proxy	Enable this option to tunnel SSH connections by a HTTP proxy. This option can be used, when the direct access to the Internet is regulated via SSH, for that SEPPmail system, however, the connection through an HTTP proxy to the Internet is possible.
Connect through Telnet proxy	Enable this option to tunnel SSH sessions through a Telnet proxy. This option can be used, when the direct access to the Internet via SSH is regulated, for that SEPPmail system, however, the connection is possible via Telnet proxy to the Internet.
Use port 80 instead of 22	Enable this option, if an HTTP connection is possible directly to the Internet. The SSH connection then uses the TCP port with destination port 80 (HTTP) instead of TCP with destination port 22 (SSH TCP/22).

»Time zone« section

Parameter	Description
Select the time zone	Select in the selection menu the system valid for the location of the SEPPmail systems. The change between summer and winter time is carried out automatically.

»Time and Date« section

© 2014 SEPPmail AG

Parameter		Description
Use current setting		With this option, the current date and the current time on the internal system is used.
Automatically synchronize with an NTP server		With this option, the date and time to the specified server is synchronized using the NTP protocol, destination port TCP/123
	Server	Host name or IP address of a time server in the network
Set date and time manually		Here you can manually enter the values for the current date and the current time.
	Date	current date in the format: dd.mm.ccyy
	Time	current time in the format: hh:mm:ss

»SNMP Daemon« section

Parameter	Description
Enable SNMP	Enable and disable the SNMP daemon on the SEPPmail system. After activating the SNMP protocols, you can use SNMP tools, such as snmpwalk, to retrieve information of your SEPPmail system. For more information on SNMP support for the SEPPmail system, see the chapter »SNMP« 51.
Listen Address	IP address, to which the SNMP monitoring connects. This is usually the IP address of the SEPPmail appliance.
Read-only Community	Password for the read-only access to the SNMP data.
Read-write Community	Password for read-write access to the SNMP data.
Download MIBs	You can download the MIB of the SEPPmail system as a ZIP file via this link.

6.4.2 Forwarding email logs to a central syslog server

To send the email log files of your SEPPmail appliance to a central syslog server, click in the configuration interface on the »System« menu item, and then click the »Advanced View« button.

Apply in the »Syslog Settings« section the name or IP address, under which the SEPPmail appliance can reach your syslog server.

6.4.3 Setting the date and time and setting up NTP synchronization

To set the date and time manually or set up automatic synchronization of your SEPPmail appliance with a Network Time Protocol (NTP) server, click on the »System« menu item in the configuration interface and then click the »Advanced View« button.

© 2014 SEPPmail AG

Use the »Time zone« and »Time and Date« sections, to define your time zone and set the date and time manually or automatically synchronize with an NTP server.

6.4.4 Enabling SNMP

To control the use of the Simple Network Management Protocol (SNMP), click in the configuration interface on the »System« menu item and then click the »Advanced View« button. To enable SNMP, click in the »SNMP Daemon« section on the »Enable SNMP« check box.

After enabling SNMP, you can use SNMP tools, such as snmpwalk, to retrieve information from your SEPPmail appliance.

© 2014 SEPPmail AG

6.5 Menu item "Mail System"

Select the »Mail System« menu item, to make the basic settings of the SEPPmail email system.

Following procedures are described in the chapters hereafter:

Overview 52
Setting up for managing email domains 58
Controlling outgoing email traffic 58
Setting up TLS encryption per email domain 58
SMTP setting 61
Email relaying 61
Antispam settings 62
Managing blacklists / whitelists 63

6.5.1 Overview of the "Mail System" menu item

»Managed Domains« section

Parameter	Description
Domain Name	List of all on the SEPPmail system applied email domains for email encryption and email routing.
Server IP Address	List of email server IP addresses for the forwarding of emails to the applied email server of the email domain.
Server Port	List of email server TCP ports on which the destination email server accepts email messages for the applied email domain.
TLS level	Indicates, which type of TLS transport encryption is to be used by SEPPmail appliance to the specified email server for each email domain.
GINA Settings	Displays the GINA profile, which has been set for this email domain.
Disclaimer Settings	Indicates, which disclaimer should be added to outgoing emails of the respective email domain.
Customer	The name of the customer, to whom this email domain has been assigned.
»Add Domain...« button	Select this button to add more email domains. These email domains must match the email addresses of your company. For more information on managing email domains, see the chapter »Setting up managed email domains« 58.
Automatically create and publish S/MIME domain keys for all domains	This parameter causes that, for all with the »Add Domain...« button newly added email domains, the will be an automatically generated self-signed X.509-S/MIME domain certificate, which is transmitted to a central update service. This newly created MIME domain certificate for your email domain is then automatically distributed to all SEPPmail systems, so that all companies which are operating a SEPPmail system, can exchange encrypted emails with each other with no additional

© 2014 SEPPmail AG

Parameter	Description
	effort. Note: If you do not want to use this, then please, disable this parameter, before you creating a new email domain. Then the S/MIME domain certificate will not be automatically generated. This process can be performed manually later using the »Generate new S/MIME Certificate« button. Such newly created S/MIME domain certificate is not transferred to the centralized update service. This paramater is enabled by default.
Fetch Mail from remote POP3 server	This parameter causes the user account, set up in the POP3 account, to be picked up by SEPPmail in a time interval. This interval is 3 minutes. The thus fetched email messages are forwarded to the local SEPPmail system. This parameter is disabled by default.
Verify recipient addresses using SMTP-Lookups	This parameter causes the recipient's email address to be verified in advance with the setup for the email domain email server to which the emails are forwarded. If the recipient email address verification is not successful, the reception of the email is denied by the SEPPmail system.

»Outgoing Server« section

Parameter		Description
Use built-in mail transport agent		This parameter causes the outgoing emails towards the Internet via the SEPPmail system to be directly delivered to the destination email server of the email recipient.
Use the following SMTP server		If you would not like the outgoing emails towards the Internet to be directly delivered, the use of an email relay server is recommend by your provider. All outgoing email messages are sent to this email relay server, which then forwards your emails towards the recipient. Alternatively, you can also use an existing internal email server for sending.
	Server name	Please enter the host name or IP address of the email relay server of your provider or the existing internal email server. Note: If you use here, according to the possibility, a host name, then IP addresses can change faster for email relay server, resulting that extra effort configuring the system can be avoided. If you use an existing internal email server, you can use its IP address, since these are not as frequently changed in internal systems.

© 2014 SEPPmail AG

Parameter		Description
Server requires authentication		Email relay server at your provider or existing internal email server usually requires a notification, so that you can transfer emails to this server. To do this, use the appropriate credentials.
	User ID	Please enter the user name to log in.
	Password	Please enter the password to log in.

»TLS settings« section

Parameter	Description
»Add TLS Domain...« button	To manage the TLS settings, choose »Add TLS Domain...« button. For more information on managing TLS email domains, see the chapter »TLS encryption for each domain Setting up« 58 .

»SMTP settings« section

Parameter		Description
max. message size (KB)		Enter in this field the maximum size of an email in kilobytes that must be transmitted through theSEPPmail system. Email messages exceeding this size are declined.
Postmaster address		Enter the email address of the local administrator of the SEPPmail system. All status messages generated from SEPPmail are sent to this email address.
SMTP server HELO string		Specify, which names SEPPmail must use in the HELO/EHLO command, when sending emails.
SMTP bind address (use with care!)		Setting the IP address of a network interface through which all emails will be received (not normally required).
openPGP key creation options		
	automatically send new public keys to users	This parameter causes the public key of the key pair generated by OpenPGP to be automatically sent to the internal users on the corporate network via email.

»Relaying« section

© 2014 SEPPmail AG

Parameter	Description
Relaying allowed: .../	Enter the IP address of the email server, from which the SEPPmail system is allowed to receive emails. You can also specify an entire IP network here.
Relaying allowed: .../	If you have a second email server, from which the emails are to be accepted, enter additionally its IP address. The SEPPmail system receives now incoming emails also from this system. You can also specify an entire IP network here.
Add Relaying for	You can enter here all other additional email servers or IP networks, from which the SEPPmail system is allowed to receive incoming emails.

»Antispam« section

Parameter		Description
Recommended Settings		If you have acquired the optional Software Option Protection Pack, Anti Virus and SPAM Protection, you will have the options to set up these optional components.
	Use Greylisting	This parameter has the effect that the »Greylisting« function is activated in the email system. Incoming external emails will not be accepted immediately, but delayed in time. This will cause the methods for the direct transmission of emails, used by spam mailers, to become unsuccessful. Using this function, you can significantly reduce the volume of SPAM emails. The reception of the desired emails is not inhibited by this function, but only delayed in time. The email server of the sender will make a new attempt to deliver after a short time. The email will then be accepted. As an external email apply to all the emails, which do not come from an email server, that are recognized under the section »Relaying«. Note: This function only works when the SEPPmail system receives incoming emails directly from the Internet. Already from another email server received and forwarded SPAM emails cannot be avoided by this function. **Note about »Greylisting«** Greylisting is a method to combat SPAM emails. With this function, it is assumed that email server and email clients comply with the RFC standard for SMTP. SPAM senders often do not use RFC compliant software to send SPAM emails. The temporary rejection of an email sent by the recipient is not evaluated and a new delivery is not done.

© 2014 SEPPmail AG

Parameter		Description
		Also through email self-spreading viruses will be rejected in this way, since they also do not make new attempt to deliver. It is recommended to use the »Greylist learning only (no mail rejection)« option for about a month before the »Use Greylisting« option is enabled. With the option »Greylist learning only (no mail rejection)« the SEPPmail appliance is in a learning mode regarding the Greylisting function and assigns no emails to be temporarily returned.
	Use Antispam Engine (Note: remember to activate in ruleset)	This parameter causes the SPAM filter to be enabled on the SEPPmail system. The configuration of the SPAM filter is carried out in the ruleset generator in the »Mail Processing« 65 menu.
	Use Antivirus Engine (Note: remember to activate in ruleset)	This parameter causes the virus scanner to be enabled on the SEPPmail system. The configuration of the virus scanner is carried out in the ruleset generator »Mail Processing« 65 menu.
	Require HELO command	This parameter verifies if the sending email server uses the HELO command, when connecting with SEPPmail. If this is not the case, no emails will be accepted while this parameter is enabled.
	PTR check (reverse DNS lookup)	SPAM senders often use email server, that are not registered in DNS. If this option is enabled, no emails will be accepted from email servers, that do not have a record in the DNS.
	Check if sender domain is valid	Use this option to enable the checking of the domain part of the sender's email address from each external incoming email. If there is no entry in the DNS for this domain, the email will not be accepted.
	Require valid hostname in HELO command	Enable this option, if emails are to be accepted only from email servers, that report with a valid host name. If there is no DNS entry for the host name, the email will not be accepted.
	Require fully qualified hostname in HELO command	Enable this option, if emails are to be accepted only by email servers, that identify themselves with a full host name (FQDN = Fully Qualified Domain Name).
	Limit incoming connections for SMTP per IP	Use this setting to limit the number of simultaneous connections per IP. This will prevent, that single servers could overload SEPPmail.
optional Settings		
	Greylist learning only (no mail rejection)	This parameter activates the greylisting learning mode. The database is set up with the information needed for the greylisting mode. Use it for about a month before you enable the active greylisting »Use Greylisting« mode.
	Strict PTR check (reserse DNS lookup)	When using this option, it is required for the acceptance of emails, that the IP address of the sending email server can be resolved in its host name in the DNS (PTR), and that the host

© 2014 SEPPmail AG

Parameter		Description
		name is pointing back to the appropriate IP address (A Record).

»Blacklists« section

Parameter	Description
Add Blacklist (RBL)	Email servers are included in blacklists due to SPAM activities. These lists are maintained by different Internet providers. To reject emails sent by such email servers, enter the name of the corresponding Realtime Blackhole Lists (RBL) in this input field.

»Manual Blacklisting / Whitelisting« section

Parameter	Description
add acccess entry	In this menu item, you can block IP networks, or explicitly permit, which email server is attempting to send an email to the SEPPmail system. Enter the IP network, the action and a comment in the corresponding input fields. network : <IP-Network or IP-Host Address> action : <Action> comment : <Comment to enter> The "action" parameter can take the following values: accept | reject accept : explicitly allow reject : block **Example:** To discard all emails sent from the IP network area 186.56.148. x, enter the IP network part 186.56.148 and define the »reject« action. Networks, from which you want to explicitly allow the acceptance of incoming emails, declare this with the »accept« action.

© 2014 SEPPmail AG

6.5.2 Setting up for managing email domains

»Mail System« menu

»Managed Domains« section

To create a new email domain, choose in the configuration interface the »Add Domain...« button.

Parameter	Description
Domain Name	Enter in the »Domain Name« field the email domain name or names, that you want to manage with your appliance. Here your domain(s) need to match the email addresses of your organization. If you have multiple email domains, register their names in the input field, separating them with a space.
Forwarding Server IP or MX name	Enter in the »Forwarding Server IP or MX name« pane the IP address or host name of the relevant email server for the email domain. Make sure that SEPPmail can access, if necessary, the corresponding email server at the IP address or the host name. The appliance will decrypt incoming emails from the defined domain(s) and forward them to the corresponding email server.
Assign to customer	Select the customer, to whom this email domain is to be assigned.

6.5.3 Controlling outgoing email traffic

»Mail System« menu

»Outgoing Server« section

If SEPPmail should send emails directly to external email recipients, select the »Use built-in mail transport agent« option. In case the external sending should take place via an existing email server, specify the appropriate server as »Outgoing Server«. If the email server requires authentication, enter the user name and password.

6.5.4 Setting up per domain TLS encryption

»Mail System« menu

»TLS settings« section

To transmit outgoing emails via TLS transport encryption, attach the email domain of the recipient. Click the »Add TLS Domain...« button.

© 2014 SEPPmail AG

Parameter	Description
Domain Name	Name of the email domain of the recipient
Optional Forwarding Server Address	IP address or host name for the recipient's email domain relevant email server

»TLS Settings« section

TLS Setting	Description
None	No TLS encryption.
May	Emails can be sent over a TLS-encrypted channel, if the receiving email server supports TLS encryption.
Encrypt	Email messages are only sent, if the transmission via TLS encryption is possible.
Verify	Email messages are sent only, if the transmission via TLS encryption is possible, and the SSL certificate of the receiving email server is valid.
Secure	Email messages are sent only, if the transmission via TLS encryption possible, and the SSL certificate of the receiving email server is valid. This test cannot be used, when using the wildcard SSL certificates. Use the TLS »Fingerprint« setting, if the email server to which you want to send emails via TLS uses a wildcard SSL certificate. If you get the »...status=deferred (Server certificate not verified)« log message, when sending an email via TLS transport encryption, check the SSL certificate of the receiving email server for the use of a the wild card certificate. The procedure is described below.
Fingerprint	Email messages are only sent, if of the transmission via TLS encryption is possible and the SSL certificate of the receiving email server matches the defined fingerprint. SHA1 is supported as fingerprint. How to read the fingerprint of an SSL certificate, is described below.

Checking the receiving email server for the use of a wildcard SSL certificate

Whether an email server uses a wildcard SSL certificate can easily be checked out with the »OpenSSL« command line tool.

Example:

```
# openssl s_client -starttls smtp -crlf -connect xxx.xxx.xxx.xxx:25
```

Replace the IP address xxx.xxx.xxx.xxx with the actual IP address of the target server, or use the host name.

© 2014 SEPPmail AG

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25
```

Here you can see the result of the query. Based on the certificate's Subject field in »CN« parameter, you can tell if this is a wildcard SSL certificate. In the response, the »CN=*.psmtp.com« value is returned. In this case it is a wildcard certificate, which can be used for all hosts in the »psmtp.com« domain. Also interesting is the »Parameter X509v3 Subject Alternative Name:«.The value is here »DNS:*.psmtp.com« returned. More domains can still be included in this field.

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25 |
openssl x509 -text -noout

  depth=1 C = US, O = Google Inc, CN = Google Internet Authority
  .
  .
  Certificate:
          .
          .
        Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=*.psmtp.
com
          .
          .
          .
                    X509v3 Subject Alternative Name:
                DNS:*.psmtp.com
```

The representation of the output was reduced to the essential information.

Reading the SHA1 fingerprint from the receiving email server's SSL certificate

One step has been described previously, as you can read the used SSL certificate from the receiving email server. It is not relevant whether this is a wildcard certificate or not.

The fingerprint of an SSL certificate can be easily read using the »OpenSSL« command line tool.

Example:

```
# openssl s_client -starttls smtp -crlf -connect xxx.xxx.xxx.xxx:25 | openssl x509
-noout -fingerprint
```

Replace the IP address xxx.xxx.xxx.xxx with the actual IP address of the target server, or use the host name.

```
# openssl s client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25 |
openssl x509 -noout -fingerprint
```

As a result, you receive the following output:

```
# openssl s client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25 |
openssl x509 -noout -fingerprint
```

© 2014 SEPPmail AG

```
depth=1 C = US, O = Google Inc, CN = Google Internet Authority
verify error:num=20:unable to get local issuer certificate
verify return:0
250 HELP
SHA1 Fingerprint=DD:9A:EC:66:E2:43:81:B9:20:2B:75:DB:30:C8:67:CC:9B:B0:D1:99
read:errno=0
```

The required SHA1 fingerprint will be displayed in the output. You can now use the configuration or take Copy & paste this value.

6.5.5 SMTP settings

»Mail System« menu

»SMTP settings« section

Parameter	Description
max. message size (KB)	Maximum size of an email message
Postmaster address	Email address of the postmaster
SMTP server HELO string	Decide which names SEPPmail should use in the HELO/EHLO command, when sending emails.
SMTP bind address (use with care!)	Set the IP address of a network interface through which all mails are received (not normally required)
OpenPGP key creation options, automatically send new public keys to users	If this option is enabled, the public keys generated by OpenPGP will be automatically sent to the users

6.5.6 Mail Relaying

»Mail System« menu

»Relaying« section

Parameter	Description
Relaying allowed	Networks or IP addresses, which can use SEPPmail as an email relay for outgoing emails. Make sure that only internal networks i.e. IP addresses, that are under your administration, are listed. This will prevent the abusive sending of emails via SEPPmail.

© 2014 SEPPmail AG

Parameter	Description
	The definition of the networks is determined by the Classless Inter-Domain Routing (CIDR) notation. This corresponds, for example the following values: • The net mask 255.255.255.255 matches "/32" (single IP addresses) • The net mask 255.255.255.0 matches "/24" (Class C network) • The net mask 255.255.0.0 matches "/16" (Class B network) • The net mask 255.0.0.0 matches "/8" (Class A network)
Add Relaying for	Enter an additional IP address, that should have a relay permission.

6.5.7 Anti-spam settings

»Mail System« menu

»Antispam« -> section »Recommended Settings« pane

Parameter	Description
Use Greylisting	Greylisting is a method for fighting spam. Here email messages are not directly accepted from unknown senders, but initially rejected. For legitimate mails, the sending mail server keeps the mails pending and submits them at a later time again. When re-attempting to deliver, the mails will then be accepted. It is assumed in this mechanism, that mail servers and clients comply with the RFC standard for SMTP. Spammers often do not use RFC compliant software for sending spam mails. They cannot cope with the errors and do not remember that they would need to try again later. Also self-propagating viruses are rejected in this way, since they also do not have a second attempt of sending. It is recommended to use the »Greylist learning only (no mail rejection)« parameter for about a month before activating the »Use Greylisting« parameter. Using the »Greylist learning only (no mail rejection)« parameter keeps the SEPPmail in greylisting learning mode and does not reject emails permanently.
Use Antispam Engine (Note: remember to activate in ruleset)	Enable this parameter to use the Protection Pack (Anti-spam / Anti-virus) for Anti-SPAM.
Use Antivirus Engine (Note: remember to activate in ruleset)	Enable this parameter to use the Protection Pack (Anti-spam / Anti-virus) for anti-virus.

© 2014 SEPPmail AG

Parameter	Description
Require HELO command	It is checked, whether the sending mail server uses the HELO command. If this is not the case, no mails will be accepted with this option checked.
PTR check (reverse DNS lookup)	Spammers are not often using in DNS registered mail server. When this option is active, no mails are accepted by corresponding mail servers.
Check if sender domain is valid	When using this option, only mails that have by the mail server specified mail exchanger host pointing to the appropriate IP address, are accepted.
Require valid hostname in HELO command	If this option is enabled, mails will only be accepted, if the mail server responds with a valid host name.
Require fully qualified domain name in HELO command	Enable this option, if only mail from those mail servers, that identify themselves with a full host name (FQDN = Fully Qualified Domain Name), should be accepted.
Limit incoming connections for SMTP per IP	Use this setting to limit the number of simultaneous connections per IP. This will prevent, that a single SEPPmail server becomes overloaded.

»Antispam« section -> »Optional Settings« pane

Parameter	Description
Greylist learning only (no mail rejection)	This option enables the greylisting learning mode. The database is set up with the information needed for the greylisting mode. Use it for about a month before activating the Use greylisting mode.
Strict PTR check (reverse DNS lookup)	When using this option, it will be required for the acceptance of mail, that the host address of the sending mail server can be resolved in DNS using its IP address (PTR), and that the name entry points again to the corresponding IP address (a record).

6.5.8 Managing Blacklists / Whitelists

»Mail System« menu

»Blacklists / Whitelists« section

Email servers are included in blacklists due to spamming activities. These lists are maintained by different providers on the Internet. To reject emails from such email servers, enter appropriate Realtime Blackhole Lists (RBL) under the heading »Blacklists«.

If you explicitly want to manually allow or block networks, enter them in the »Manual Blacklisting / Whitelisting« section.

To discard for example, all emails from the network 186.56.148.x, specify 186.56.148 and define the » reject« action. Networks from which you want to explicitly allow the acceptance of emails, you

© 2014 SEPPmail AG

declare other hand with the »accept« action.

© 2014 SEPPmail AG

6.6 "Mail Processing" menu item

This chapter describes the management of the email rules.

Following procedures are described in the sections hereafter:

GINA web mail interface 65
Creating GINA webmail domains 66
Deleting GINA webmail domains 66
Managing GINA webmail domains 66
Managing GINA webmail layout 72
Managing GINA webmail language support 75
GINA self service password management 80
GINA internal encryption 80
Processing rules of webmail managing 82
Managing webmail password SMS sending 84
Managing disclaimer 87
Managing email templates 88
Managing rulesets 89
Remote webmail relay 101
Viewing rulesets 102
Loading ruleset 102

6.6.1 GINA web mail interface

GINA is the new standard interface for secure web mail. With version 6 sets SEPPmail a new secure email standard. The transmission of digitally signed and encrypted emails is easier than ever - for senders and recipients alike.

The secure email platform SEPPmail V6 GINA may be called the simplest, the most versatile and yet the most convenient solution for highly secure email transmission of the world. It impresses with numerous highlights.

Contemporary user interface
- intuitively operable user interface
- Maximum comfort, when receiving and opening secured emails via web mail
- User friendly integration of mobile devices

Portal functions
- External users have the option to send encrypted emails at any time to internal employees
- External users can register independently via portal
- Pre-existing keys (S/MIME oder PGP) can be independently uploaded by external users

Customizing - Adjusting the layout to your needs
- Adaptation of all the GINA components to individual needs - for example, to implement the implementation of corporate design guidelines
- Integration into company websites, portals etc.
- Integration of any languages (ideal for international companies as well as for cloud service providers)

Self Service Password Management (SSPM)
- Forgotten passwords can be re-generated i.e. requested by the recipient via mobile phone automatically and without security risks.

Inline Encryption (IME)

© 2014 SEPPmail AG

- Comfortable, internal encryption of confidential emails - from the workplace of the sender to the desktop of the recipient; thereby confidential emails are protected from unauthorized access throughout the corporate network

6.6.1.1 Creating GINA domains

»Mail Processing« menu

In order to create a new GINA domain, click the »GINA domains« section on the »Create new GINA domain...« button.

»Create new GINA Domain« section

Parameter	Description
Description	a description of the new GINA domain
Host name	Host name of the new GINA domain. This name is part of the URL, which is available for calls from web mail, e.g. https:// secmail.cusomer.com/customer

Confirm the creation of a new GINA domain by clicking on the »Create« button.

6.6.1.2 Deleting GINA domains

»Mail Processing« menu

To delete an existing GINA domain, select the GINA domain in the »Mail Processing« menu -> »GINA domains« and click the »Delete« button.

Confirm the deletion of an existing GINA domain by clicking on the »Delete« button.

6.6.1.3 Managing GINA Domains

»Mail Processing« menu

You can edit GINA settings by pressing the corresponding GINA domain in the »GINA domains« section and click the Edit... button. The default GINA domain has the name [default].

© 2014 SEPPmail AG

You can manage parameters in the following categories:

- Hostname 67
- Secure Webmail Port 67
- Secure Webmail Key and certificate 67
- Master Template 67
- Admin 67
- Extended settings 67
- Terms of use 70
- Language settings 70
- Security 70
- Certificate login 72

These sections are explained in detail hereafter.

»Secure GINA Host« section

In the »Secure GINA Host« section, you can define values for Hostname, Port, Key and certificate of the GINA domain. This host name is part of the URL, downloaded from the GINA messages, e.g. https://secmail.customer.com. If you have enabled the »Virtual Hosting« function, you can assign a specific port and deposit own SSL certificate for each GINA domain.

»Master Template« section

This section is not displayed, when you select the GINA domain [default].

In the »Master Template« section, select the GINA domain, that you want to use as a template. The settings are inherited by this GINA domain. This simplifies the management of options, which you should have for multiple GINA domain validity.

When selecting the default GINA domain [default], it is used as a template to assume the settings. Set the extent, to which settings are to be applied, in the individual sections, which are explained in detail below.

»Admin« section

In the »Admin« section you can enter an email address for the administrator who receives a notification email, if a GINA recipient would like to have his/her password reset. To do this, the security level must be set to »Reset by hotline«.

»Extended settings« section

Parameter	Description
Use settings from master template	Select this check box, if you want to apply the settings from the master template.
Default Forward Page	URL that is used if the GINA user interface is directly calling, instead a GINA message (optional).
Always zip HTML attachments, when encrypting mail with GINA technology (for OWA	Use this setting, when the encrypted email part of a GINA message is to be attached in ZIP format, instead of HTML format. This setting is required, if the recipient uses Outlook Web Access (OWA), since the GINA messages in HTML format

© 2014 SEPPmail AG

Parameter	Description
compatibility, for single mails use [owa] in subject)	cannot be deciphered from OWA. To use the setting only for individual emails, the term [owa] can be used as a control statement in the subject line. If a GINA message in HTML format arrives to an OWA recipient, the SEPPmail appliance recognizes this. The sender is prompted to resend the email again. At the same time, the GINA user account of the recipient will become activated with the »Zip Attachment« parameter. The recipient can easily read a GINA message created with this setting.
"Send copy to myself" checked by default, when writing GINA mails	This setting causes for the GINA users the activation of »send copy to myself« option (copy of outgoing e-mails send to itself) by default.
Sender always receives notification, when recipient reads mail in web viewer (overrides user setting)	Enable this setting to receive a notification, when an a recipient opens and reads a GINA message in the GINA portal. The user-specific settings are overwritten.
Allow account self-registration in GINA portal without initial mail	Enables the registration of a new GINA recipient without this having received a GINA message before. The user can register himself via the GINA portal as GINA recipient. The user receives a confirmation via email with an activation link. After confirming the activation link, the new GINA user account can be used. For more information, see the chapter GINA self-registration through web mail portal 78.
Enable S/MIME certificate / PGP key search and management in GINA	Allows a GINAuser to additionally store an existing PGP or S/MIME public key in the certificate store of the SEPPmail appliance. The GINA user can then also receive encrypted emails via PGP or S/MIME. For more information, see the chapter GINA S/MIME and PGP key search through web mail portal 81. You must enable this option in order to enable the following option »Allow unregistered users to search public keys/certificates of internal users«. Otherwise, the following option cannot be activated.
Allow download of public domain keys/domain certificates (Note: You must assign "Use GINA Settings" under Mail System Settings / Managed Domains)	Allows external unregistered users to independently search and download existing PGP or S/MIME domain keys of the applied managed domains via the GINA portal.
Allow unregistered users to search public keys/ certificates of internal users (and domain keys, if enabled above)	Allows external unregistered internal users to independently search for and download existing PGP or S/MIME public keys via the GINA portal.

© 2014 SEPPmail AG

Parameter	Description
Allow GINA users to write new mails (not reply)	Enable this setting, when the button to create new emails in the GINA portal should be active. A GINA user can then send emails to internal staff from the GINA portal. You can use this function to send messages only to internal staff email addresses. The email sending to external email addresses is not possible.
Do not allow GINA users to edit recipient when replying to emails	Enable this parameter, if you want to ensure that when responding to a GINA message, the recipient's email address can be changed.
Allow messages to be downloaded as Outlook message (.msg) files	Enable this setting if the Outlook button should be displayed in the GINA frontend. You can then use the decrypted emails in Outlook format ".msg", save in the local file system and subsequently import them into Outlook. The message is stored in plain text.
Allow messages to be downloaded as MIME (.eml) files	Enable this setting, if the button to Save message should be displayed in the GINA front end. You can then save decrypted emails in the local file system in standard ".eml" format and subsequently import them into an email client. The message is stored in plain text.
When encrypting mail with GINA technology, use text-only emails (no HTML emails)	The short information note for the GINA recipient is running as text only message and not as HTML message.

»Large File Management« section

Parameter	Description
Enable Large File Management	Enables or disables the »Large File Management« function.
Days to store Large Files	Time in days to store the cached files.
Threshold for Large Files	Size of the email in KB for an email, that is processed via »LFM«.
Limit Large Files per Day	Number of files, that a user can send per day via »LFM«.

© 2014 SEPPmail AG

For the operation of Large File Management, it is necessary to set up additional area on the local data memory. This area is displayed in the »Home« menu as »LFM store«.

To set up the additional data storage for Large File Management, contact your support.

»Terms of use« section

Parameter	Description
Use settings from master template	Select this check box, if you want to apply the settings from the master template.
Require new users to accept terms of use	Select this check box, if you want that each new GINA user first activating their GINA user account must accept the specific use conditions. The detailed terms of use may be consulted at the registered URL.
Terms of use URL (required)	Enter here the URL, under which the terms of use can be viewed on the Internet. (for example http://www.customer.com/termsofuse.html)

»Language settings« section

Parameter	Description
Default language	Set the default language for the GINA portal
Available Languages	Enable, disable, and add existing and/or new languages Learn more about this in Chapter Managing GINA Webmail Language Support 75.

If you want to copy the settings from the master template, click the check box »Use settings from master template«. This option is only visible, if you are in the process of configuration of an additionally created GINA domain.

»Security« section

Parameter	Description
Choose how the user can retrieve lost passwords	Defines the standard procedure for a password reset within the GINA domain
Minimum password length	Defines the minimum length of a password
Password Complexity	Defines the complexity of the password

»Choose how the user can retrieve lost passwords« parameter

Select the method for password reset, so that external GINA users can reset their GINA user

© 2014 SEPPmail AG

password. Thereafter, depending on the selected method for password reset, one of the following methods is used:

»default (Reset by hotline)« selection value

The »default« value refers to the respective GINA domain selected global default. This is set within the configuration GINA domain in the »Security« section.

»Reset by Email verification« selection value

The external GINA users can reset their password themselves. To activate and confirm the action, they receive an email notification with an activation link. After confirming this external user activation link, the newly entered user password is enabled. A login with the newly set password is now possible.

»Reset by hotline« selection value

The external GINA users cannot reset their password automatically. They give for that purpose their phone number, under which they can be contacted for support. After review by the security question, they receive a new one-time password from the support staff for next login. After logging in, it is necessary to record a new personal password. A login with the newly set password is now possible.

»Reset by hotline, no reminder question/answer« selection value

The external GINA users can not reset their password automatically. They give for that purpose their phone number, under which they can be contacted for support. A review by answering a security question is not required. When initializing a GINA user account the first time it is not required, that the user specifies a security question. The user receives a new one-time password from the support staff for next login. After logging in, it is necessary to record a new personal password. A login with the newly set password is now possible.

These following options for a password reset can be performed only within the Self Service Password Management (SSPM) function. See GINA Self Service Password Management 80

»Reset by SMS« selection value

The external GINA users can request a new password via SMS to their mobile phone. This new one-time password is used by the user for the next login. He must record a new personal password. A login with the newly set password is now possible.

When resetting the password via SMS, the mobile phone number must have been stored in the user profile of the user.

Including in a selected method for password reset, the SMS option, it is also required that set up of the SMS sending is done in the »Mail Processing« menu.

»Let user choose between hotline and SMS« selection value

The external GINA users may choose to request a new password between the two options »Hotline« and »SMS«.

»Mobile Number« parameter

© 2014 SEPPmail AG

Includes the GINA users' mobile telephone numbers, if they were stored by users while managing ther accounts. It is possible for the support purposes for the user, if necessary, to send a new one-time password (OTP) via SMS. Click on the »SMS password reset«. A new one-time password is automatically generated by SEPPmail by and sent via SMS.

»Minimum password length« and »Password Complexity« parameters

Parameter	Description
Minimum password length	Minimum password length (default: 8 characters)
Must contain at least one lower case letter	The password must contain at least one lowercase letter.
Must contain at least one upper case letter	The password must contain at least one uppercase letter.
Must contain at least one number	The password must contain at least one numeric character.
Must contain at least one special character	The password must contain at least one special character.
Must not contain own name or mail address	The password must not include your own name or your own email address.
Must be different from previous password	The password must not be the same as the previous one.

If you want to copy the settings from the master template, click the check box »Use settings from master template«.

»Certificate login« section

In the »Certificate Login« section you can deposit a root CA certificate (e.g. SuisseID) of the GINA user, that can be used for user identification. Each GINA user must have in their web browser a certificate installed, that was issued before the one stored here as root CA.

If you want to copy the settings from the master template, click the check box »Use settings from master template«.

6.6.1.4 Managing GINA Layout

»Mail Processing« menu

To customize the layout of an existing web mail domain, choose from the configuration menu of the GINA domain the »Edit GINA Layout« button. You are now in the configuration for the GINA layout of the respective GINA domain.

© 2014 SEPPmail AG

You can manage parameters in the following categories:

Header Logo 73
Company Logo 73
Favorites Icon 73
Footer Logo 73
Background Image 73
Web mail CSS 73
Extended settings 73

»Header Logo« section

In this section you can add an additional graphics in the »Header Logo« pane to be embedded in the web mail interface. The display of this graphics is activated in the Extended Settings 73 section.

»Company Logo« section

To adjust the GINA user interface to adopt corporate design guidelines, you have the option to insert a company logo in this section. Further adjustments can be made in the default CSS file of the GINA user interface. See Managing GINA web mail layout 73

»Favourites Icon« section

In this section you can connect an optional favicon in the file format .ico. This favicon is displayed as a graphic at the beginning of the address line of the web browser.

»Footer Logo« section

In this section, you can embed an additional graphics element in the »Footer Logo« pane of the GINA user interface. The display of these graphics is activated in the Extended Settings 73 section.

»Background Image« section

In this section you can insert a picture as background for the GINA user interface. You can manage other features in the Managing GINA web mail layout 73 section.

»GINA CSS« section

In this section you can manage all GINA properties. A CSS file is used to customize the layout of the GINA interface. This way the data and the formatting are separated. When you can deal with the CSS, you can customize the GINA user interface e.g. embed your corporate requirements etc. to easily integrate it into your website.

»Extended settings« section

In this section, you can enable or disable the previously set up options for displaying in the GINA user interface.

Parameter	Description
Disable "Powered by ..." Logo in web mail viewer	When enabled, the text "Powered by SEPPmail" message is not displayed when calling a GINA message.

© 2014 SEPPmail AG

Parameter	Description
Enable header logo on login page	enable the header logo inside the GINA log on
Enable header logo on all other pages	enable the header logo throughout the GINA user interface
Enable footer logo on Login page	enable the footer logo inside the GINA log on
Enable footer logo an all other pages	enable the footer logo throughout the GINA user interface
Enable footer text an login page	enable the footer text inside the GINA log on
Enable footer text on all other pages	enable the footer text throughout the entire GINA user interface

The settings for the footer test can be found in the section Manage GINA web mail language support 76.

© 2014 SEPPmail AG

6.6.1.5 Managing GINA language support

In the »Language Settings« section, you have the possibility to customize the translations included in delivery or to add your own translations for additional language support to the GINA user interface.

You can make the following settings in this section:

Edit translations... 75
Download 77
Add new... 77

Parameter/Button	Description
Default language	Setting the default language for the GINA user interface
Available Languages	Download and customize an existing language version for GINA user interface
Edit Translations button	Customizing the translation of an existing language version
Download button	Download the latest translation of the language and possibly use as a template for your own translations
Change button	Save the changes made in this section
Add new button	Add translation for a new language variant

The following translations are included in the delivery:

- English - English (e)
- Español - Spanish (s)
- Deutsch - German (d)
- Français - French (f)
- Italiano - Italian (i)

If you want to copy the settings from the master template, click the check box »Use settings from master template«. This option is not visible in the settings of the default web mail domain » [default]«, but appears only in additionally created web mail domains.

»Edit translations...« button

© 2014 SEPPmail AG

You can customize current translation via the »Edit translations...« button for the actual translation of certain text of the GINA user interface itself and text of the short textual description of the GINA message.

Within this section, you can navigate with the following buttons:

Back	: Return to the parent configuration page
Advanced View	: Expands the view and enables the processing of further resource records of the translation
Normal View	: is only available, if the »Advanced View« button has been previously pressed

The following text components can be edited:

Customization 76
Text in Secure Web mail 76
Open hint in Secure Web mail 76
Greeting on Login page 76
Footer text 76
Webmail Password Notification Mail 77

In the advanced view:

Edit Translation file 77

»Customization« section

Important notice

- Do not use any of the reserved keywords »msgid« and »msgstr« in any part of the text.
- Text must not contain any blank lines in order to create a line break. Use skip to generate a line break. Each <br> is replaced by a newline. (e.g., as in plain text emails).
- HTML TAG's are not allowed. You may only use within text components, that are displayed in the Webmail Viewer.

»Text in GINA« section

This text is displayed inside the GINA message as short information text and contains instructions for handling this email to the recipient.

»Open hint in GINA« section

This text is displayed in the login dialog, when you open a web mail and sign up for decryption.

»Greeting on Login page« section

Welcome message after you open a GINA message to decrypt.

»Footer text« section

© 2014 SEPPmail AG

This text is displayed in the footer area of the GINA interface and can be turned on and off. See Managing GINA web mail layout 73.

»GINA Password Notification Mail« section

This text is inserted into password notification received by a sender, after a GINA message has been sent to a recipient the first time.

»Edit Translation file« section

Select the »Advanded View« button to get the editor to translate the language version, that you selected.

In this section you can edit the translation of the language, that you selected. To hide this field, select the »Normal View« button.

»Download« button.

By pressing the »Download« button you can download the latest translation of an existing language version and use this as basis for a new translation of an additional language variant.

»Add new...« section

To add the translation for a new language support, select the »Add new...« button. You can enter the following parameters:

Parameter	Description
Name	Name the new language in the local language, e.g. Polski for Polish
Please enter the name of the new language for all available languages	Add the translation of the existing languages in the new language variant, e.g. Deutsch, German, Allemand, Tedesco, Alemán etc. for German. These are mandatory fields.
Please optionally select an identifying letter for the new language	Give the new language version a letter.
Please upload the complete translation file for the new language	Select the resource file with the complete translation for the new language version to upload.

© 2014 SEPPmail AG

6.6.1.6 GINA self registration through web mail portal

To register your own GINA user account, it is necessary to connect to the GINA portal on the web browser. You can access the GINA portal via the following link:

/web.app

External users have the possibility to register themselves via the GINA portal as GINA users. To register as an external user, proceed as described in the following steps:

Step 1

Sign up as GINA user on your SEPPmail system. On the GINA portal, access from web browser the following link:

/web.app

The placeholder <SecureWebmailAppliance> stands for the IP address or host name in which the SEPPmail system is internally accessible.

In order for the pane »Register new account« to appear in the GINA Secure web mail portal, it is necessary to select in the menu »Mail Processing -> [Webmail-Domain]« in the section »Extended Settings« the option »Allow account self-registration in web mail without initial mail« for activation. See Managing GINA Webmail-Domains 67

Step 2

Choose in the »Register new account« pane the »Registration« button to create a user account.

Select the »Continue« button to proceed. Confirm the following dialog with the »Save« button. You will then receive a confirmation email with an »Activation-Link«. By selecting this link, you confirm registration. The user account is now active and you can log on. To do this, use the data specified when registering for your username and password. (User name = email address)

Step 3

Confirm the activation link in the confirmation email.

The newly created GINA account has now been activated and can be used.

Step 4

Log on with your login data.

After successful login to your new GINA account, you can manage your account or compose a new GINA message. For more information, see the menu Managing GINA Web mail account 79.

© 2014 SEPPmail AG

6.6.1.7 Managing GINA Accounts

To manage the own GINA user account, it is necessary to connect to the GINA portal via the web browser. Accessed via the following link for GINA portal:

/web.app

For the administration of a GINA user account, the following buttons are available:

Write email 79
Profile 79
Edit profile 79
Change password 79
Keys/Certificates 79

»Write email« button

Select the »Write email« button, to create a new GINA message. Your own email address will be used as the sender. As a recipient, you can use all email addresses that are set up for email routing of the SEPPmail system. This involves all the internal email addresses, that the SEPPmail system operates.

It is not possible to use GINA messages to any external recipients on the Internet. The relay permission applies to all internal email domains.

»Profile« button

Select the »Profile« button to see the own profile data.

»Edit profile« button

Select the »Edit profile« button to change your profile data. You can modify the following data:

- Name
- Language version of the web mail interface
- Mobile phone number

»Change password« button

Select the »Change password« button to set a new password and security question to recover a password.

»Keys/Certificates« button

Select the »Keys/Certificates« button upload your own S/MIME public keys or PGP public keys for SEPPmail system upload. These certificates and keys can be used in the future to send your MIME or PGP encrypted emails.

You also have the option of downloading S/MIME or PGP public keys from internal employees to send also them S/MIME or PGP encrypted emails.

© 2014 SEPPmail AG

6.6.1.8 GINA Self Service Password Management

The function »Self Service Password Management (SSPM)« enables requesting the forgotten passwords of the respective recipient via mobile phone to be regenerated automatically i.e. without security risks.

This function is optionally available. You will need a separate license. Whether your SEPPmail system is already licensed for use system, you can see in the »Home« menu in the »License« section.

To use this feature, follow these steps:

Open a previously issued GINA message. In the login dialog, click the »Forgot your Password?«

You will obtain a selection of ways you can reset the password. Depending on the security settings for password reset, you will be offered the following options:

You have the framework of the function »Self Service Password Management (SSPM)«, in addition to the following default features, to reset the password:

Parameter	Description
default (Reset by hotline)	For default, see Managing GINA web mail domains 70
Reset by Email verification	For default, see Managing GINA web mail domains 70
Reset by hotline	For default, see Managing GINA web mail domains 70
Reset by hotline, no reminder question/answer	For default, see Managing GINA web mail domains 70

These following options for a password reset can be performed only within the function »Self Service Password Management (SSPM)«.

Parameter	Description
Reset by SMS	the web mail user will receive a new password via SMS, if the security question is correctly answered, then the web mail user needs to select a new password and save
Let user choose between hotline and SMS	the webmail user has the option to select the password reset option between the hotline and SMS

6.6.1.9 GINA internal encryption

The function of Inline Encryption (IME) allows confidential emails to be comfortably sent encrypted within the company - from the workplace of the sender to the recipient's desktop of. As a result, confidential internal emails throughout the corporate network are protected against unauthorized access.

This function is available on option. You will need a separate license. To check, whether your SEPPmail system is already licensed for use, see in the »Home« menu in the »License« section.

© 2014 SEPPmail AG

To use this feature, follow these steps:

Step 1

Sign up as internal GINA user on your SEPPmail system. On the GINA portal, access the following link via web browser:

/web.app

The placeholder <SecureWebmailAppliance> stands for the internally accessible IP address or host name in the SEPPmail system.

In order for the pane »Register new account« to appear in the web mail interface, the »Mail Processing -> [Webmail-Domain]« menu item in the »Extended Settings« section and the »Allow account self-registration in web mail without initial mail« option must be activated. See Managing GINA web mail domains 67

Choose in the »Register new account« pane, the »Registration« button, to create a user account.

Select the »Continue« button to proceed. Confirm in the following dialog, using the »Save« button. You will then receive a confirmation email with an »Activation-Link«. By selecting this link, you confirm registration. The user account is now active and you can log on. To do this, use the data specified when registering your user name and password. (User name = Email Address)

Step 2

After successful registration, you can send emails to internal users from your new GINA account. The recipients will receive your message as encrypted GINA message in their mailbox. The message remains, even after reading, still encrypted in the recipient's mailbox.

6.6.1.10 GINA S/MIME and PGP key search via GINA Portal

External users have the option to find themselves S/MIME or PGP public keys from the GINA portal from internal staff and to download them. It is also possible to search for S/MIME or PGP public key certificates for the domain encryption and to download them.

To access the GINA portal via a web browser, use the following link: /web.app

The placeholder <SecureWebmailAppliance>is the IP address or host name where the SEPPmail system is internally accessible.

In order to display the »Search Keys/Certificates« pane in the GINA portal, must the »Mail Processing -> [Webmail-Domain]« menu item in the »Extended Settings« section of the »Allow unregistered users to search public keys/ certificates of internal users« parameter be enabled. See Managing GINA web mail domain 67.

In order to display the »Search Keys/Certificates« pane only for registered users, the »Enable S/MIME certificate / PGP key search and management in webmail« option must be enabled.

© 2014 SEPPmail AG

6.6.2 Managing rules for the processing of GINA messages

»Mail Processing« menu -> »GINA settings« section

Parameter	Description
Password Length	Length of the automatically generated by passwords (default: 8 characters) via Enhanced Secure Webmail (0 = passwords are not generated automatically, but set by the recipient of the GINA message)
Use virtual hosting	Defines the appearance of the URL to access the GINA portal while adding additional GINA domains
Secure GINA track access (e.g. http://192.168.1.60:8080)	Address of the web application for displaying the read status of a GINA message

In the default behavior, the GINA uses per-applied GINA domain an independent URL for accessing the GINA portal.

Example:

There are three GINA applied domains. Each GINA domain has its own portal configuration. The respective GINA portals can be accessed via an independent URL.

https://secmail.customer1.com/web.app
https://secmail.customer2.com/web.app
https://secmail.customer3.com/web.app

The FQDNs stated in the example are specified as the host name within the respective GINA domain.

Example:

Hostname: secmail.customer1.com

The default behavior can be changed by the following parameters.

»Use virtual hosting« parameter

Enabling this parameter is required, if additional GINA domains must be created and the respective GINA portal for the additional domains via an independent URL should be reachable.

Default behavior without additional GINA domains and without activated »virtual hosting«

Example:

GINA-Hostname [Default]:
secmail.customer.com

GINA URL embedded in the secure webmail [default]:
https://**secmail.customer.com**/web.app?op=init

Default behavior with additional GINA domains and without activated »virtual

© 2014 SEPPmail AG

hosting«

```
Example:

GINA-Hostname [Default]:
   secmail.customer.com

GINA URI embedded in the secure webmail for [default]:
   https://secmail.customer.com/web.app?op=init


GINA-Hostname [customerDomain1]:
   secmail.customer1.com

GINA URI embedded in the secure webmail for [customerDomain1]:
   https://secmail.customer.com/secmail.customer1.com/web.app?op=init
```

In this example, you can see that without »virtual hosting« the GINA portal of the additional GINA domain as a path below of the [Default] GINA domain will be used. In order to optimize this behavior, it may be useful to not to use separate FQDN as the host names for the additional domain, but to use a simple path name.

```
Example:

GINA-Hostname [customerDomain1]:
   mypath

GINA URI embedded in the secure webmail for [customerDomain1]:
   https://secmail.customer.com/mypath/web.app?op=init

Replace the »mypath« path by a suitable value for you.
```

Behavior with additional GINA domains and MIT activated »virtual hosting«

With activated »virtual hosting«, the GINA portals are accessible from the additional GINA domains via an independent URL. Within each additional GINA domain, a unique FQDN must be registered as host name.

```
Example:

GINA-Hostname [Default]:
   secmail.customer.com

GINA URL embedded in the secure webmail [default]:
   https://secmail.customer.com/web.app?op=init


GINA-Hostname [customerDomain1]:
   secmail.customer1.com

GINA URI embedded in the secure webmail for [customerDomain1]:
   https://secmail.customer1.com/web.app?op=init
```

Parameter »Secure GINA track access«

© 2014 SEPPmail AG

This function makes it possible to provide a differentiated feedback read receipts for sent GINA messages. If a GINA sends a message with read receipt request to multiple recipients, only the first read receipt is sent back to the sender. In addition, the read receipt contains a link to the complete list overview of read receipts. This link starts with the address, which is input to the field. The rear part of the link is dynamically generated.

Example:

http://192.168.1.60:8080

Feedback to the sender
http://192.168.253.60:8080/track.app?track=$MjAxMzA3Mj...

6.6.3 Managing GINA SMS password transmission

»Mail Processing« menu -> »GINA password via SMS« section

General information on SMS transmission of the GINA password notifications

The GINA interface makes it possible to transmit, as the first time dispatch a GINA message with the password notification via SMS to the recipient.

This process can be simplified by using the mobile phone number to send the password notification as part of the subject of the GINA message. The mobile phone number is removed from the subject before transmission via SEPPmail to the Internet.

You have the following options to submit the password notification via SMS:

- As part of the email subject line

  Insert (mobile: +49123456789) or (sms: +49123456789) in the subject

  Example:

  Subject: Secure email encryption (mobile: +49123456789)
  Subject: Secure email encryption (sms: +49123456789)

- Use a mobile phone number previously stored in the GINA user account

  In the GINA user account stored mobile phone number can be used for the »Self-Service password management« function. External GINA users have the ability to reset their own user password automatically when needed.

- Send a one-time password (One-Time Password) via the configuration interface in the »GINA accounts -> [name of GINA user account]« menu

  This option is typically used by an administrator to reset the user password.

- Using a web application (default) integrated in SEPPmail

  For internal users, an integrated web application for sending SMS messages to new external GINA users can be set up. This web application can be accessed either via the configuration web server or the public GINA portal.

© 2014 SEPPmail AG

Different configuration options to set up the interface for sending SMS messages are available at SEPPmail. This is a globally effective configuration, that cannot be influenced by the user.

Parameter	Description
Disable	Disable SMS dispatch
Use cell phone / GSM modem attached to appliance	Use a mobile phone or GSM modem, which is connected directly to the hardware appliance
Use Mail to SMS service (configuration below)	Use email-to-SMS Gateway service, or with the following settings
Use xml service (configuration below)	XML Service (for more information, please contact the technical support)
Use HTTP GET service (configuration below)	HTTP GET service (for more information, please contact the technical support)

Depending on the selected option for sending SMS, you can make detailed configuration.

The following variables (placeholders) are available within the configuration for the XML service and the HTTP GET service:

1. `$sms` : to transmit the message text
2. `$number` : Mobile phone number including country code (+xx...)
3. `$countrycode` : Country code, e.g. "49"
4. `$localnumber` : Mobile number WITHOUT the country code

»Use cell phone / GSM modem attached to appliance« parameter

For this parameter no detailed configuration is available. When using a hardware appliance, there is the option of connecting a mobile phone via USB cable. This control is achieved automatically by the SEPPmail system.

»Use Mail to SMS service« parameter

Mail from:
Sender email address for the SMS dispatch

Gateway Domain <Mobile #>@:
Gateway domain for the SMS dispatch

»Use xml service« parameter

Here you are binding an XML service of an external service provider to send GINA Password notifications via SMS. For this purpose, the following parameters are available:

Server address:
Address of the external server to which the XML template should be transmitted. You can get this address from your service provider.

© 2014 SEPPmail AG

XML example: https://xml1.aspsms.com

xml template:
Source code for the XML template. You get this information from your service provider.

XML example:

```
<?xml version="1.0" encoding="UTF-8"?>
<aspsms>
      <Userkey>xyz</Userkey>
      <Password>xyz</Password>
      <Originator>Secmail</Originator>
      <FlashingSMS>1</FlashingSMS>
      <Recipient>
            <PhoneNumber>$number</PhoneNumber>
      </Recipient>
      <MessageData><![CDATA[$sms]]></MessageData>
      <Action>SendTextSMS</Action>
</aspsms>
```

»Use HTTP GET service« parameter

Here you link up the HTTP GET service of an external service provider to send GINA password notifications via SMS. For this purpose, the following parameters are available:

Server address:
Address of the external server, where the HTTP GET String is to be transmitted. You can get this address from your service provider.

HTTP Get example: https://www.chrus.ch

HTTP Get String:
Pathname with usage including the parameters with to be transmitted via SMS data.

HTTP Get example: /mysms/http/send.php?
user=xyz&pwd=xyz&from=Secmail&to=$number&msg=$sms

Permission to access the built-in web application for the SMS transmission

Parameter	Description
Disabled	Access to the web application for the SMS transmission is disabled
Available via public GINA GUI	Enables access to the web application for sending SMS of password notifications vie the public GINA portal. The web application is available on the same port than the GINA Portal. (Default: TCP/443 - HTTPS)
Available via the following URL (e.g. https://192.168.1.60:8443/pwsend.app)	Enables access to the web application for sending SMS of password notifications from the internal network. The web application is available on the same port, than the configuration interface. (Default TCP/8443)

© 2014 SEPPmail AG

Access to GINA send password form:

»Available via public Webmail GUI« parameter

To send a password notification via SMS, the internal sender receives an email message. This password notification will be, when creating a GINA account for an external recipient, automatically generated and sent to the internal sender. This email message contains a link to a web application, via which the SMS transmission is performed. Depending on the individual implementation of the Enhanced Secure Webmail systems, it may be required to access this web application from the public GINAportal. Enable this option to access the port of the web application via the GINA portal. It is recommended to use the default port for HTTPS (TCP/443).

Example:

GINA portal accessible via:
https://secmail.customer.com/web.app

Web application for the SMS transmission of the password notification available via:
https://secmail.customer.com/pesend.app

»Available via the following URL« parameter

To send a password notification via SMS, the internal sender gets an email message. This password notification is automatically generated and sent to the internal sender when creating a GINA account for an external recipient. This email message contains a link to a web application via which the SMS transmission is to be performed. The web application is accessible only via the URI, defined in this input field. This setting can be used, when the web application to be accessible only from the internal network.

Example:

Web application for the SMS transmission of the password notification available via:
https://192.168.1.60:8443/pwsend.app

6.6.4 Managing Disclaimer

»Mail Processing« menu -> »Edit Disclaimer« section

The standard disclaimer is named [default]. Below, you can add an additional disclaimer besides the standard disclaimer and configure, delete a disclaimer or edit an existing Disclaimer.

Deleting a disclaimer

© 2014 SEPPmail AG

To delete a disclaimer, select the disclaimer to be deleted and click on the »Delete...« button. The disclaimer is removed from the configuration.

Please note, that this disclaimer will no longer remain within the ruleset programming, before you delete it. Otherwise, it may cause problems in the execution of the ruleset statements.

Editing an existing disclaimer

To edit an existing disclaimer, click the »Edit...« button.

»Disclaimer as text« parameter

Include in this field the contents of the disclaimer in plain text format.

»Disclaimer as Html« parameter

Include in this field the content of the disclaimer in HTML format. You can use different HTML tags for formatting here. (E.g. paragraphs, font size or font color)

Creating a new disclaimer

They can set up additional disclaimer, if required, in addition to the standard disclaimer named [default]. A disclaimer can be assigned and used within the configuration of a »Managed Domain« The disclaimer is automatically appended to all outgoing emails of this »Managed Domain«.

To set up an additional disclaimer, click the »Create new disclaimer...« button. Enter a name for the new disclaimer, and click the »Create« button. Then select your new disclaimer, in the selection list and click on the »Edit...« button. You can now edit the text of the new disclaimer.

6.6.5 Managing email templates (Templates)

»Mail Processing« menu -> »Edit Mail Templates« section

Templates are predefined messages, that are automatically sent in defined circumstances. Templates can be used only within the ruleset statements.

Managing the »bounce_noenc« default template.

The only template, that is available after commissioning of the SEPPmail system, has the designation »bounce_noenc«. This template is used, when a sender tries to send an encrypted email, but the encryption, however, fails. The email is not, in such a case, sent via Enhanced Secure Webmail. The sender will receive a notification by email with the content of the template as the message body.

To edit the »bounce_noenc« template, click on the »Edit...« button.

© 2014 SEPPmail AG

Deleting a template

To delete a template, select the template you want to delete and click the »Delete...« button. The template is removed from the configuration.

Please note, that this template will no longer be available within the the ruleset programming, before you delete it. Otherwise, it may cause problems in the execution of the ruleset statements.

Editing an existing template

To edit an existing template, click the »Edit...« button.

»Template as text« parameter

Include the contents of the template in this field in text format.

The following variables (placeholders) are available within the configuration for the template:

1. $to : Recipient's email address
2. $header_to : Header of the original email as an attachment

Creating a new template

You can set up additional templates, in addition to the default template, if required, with the name »bounce_noenc«. A template is used in each case by an appropriate ruleset statement.

To set up an additional template, click the »Create new template...« button. Enter a name for the new template and click the »Create« button. Then select your new template in the list and click on the button »Edit...« button. You can now edit the text of the new template.

6.6.6 Managing rulesets

»Mail Processing« menu -> »Ruleset Generator« section

The »Ruleset« section is divided into the following areas:

1. General Settings 90
2. User Creation 90
3. Encryption / Decryption 92
4. Signing 95
5. Key Generation 97
6. Protection Pack (Anti-SPAM / Anti-Virus) 98
7. Header tagging 99
8. Archiving 100
9. Custom Commands 100
10. Advanced Options 101
11. Remote Webmail Relay 101

These areas are explained in detail below.

© 2014 SEPPmail AG

»Ruleset Generator« section -> »General Settings« pane

Parameter	Description
Do not touch mails with the following text in subject	Define a tag to prevent the cryptographic processing of an email.
Add disclaimer to all outgoing emails	Adds the standard disclaimer to all outgoing email messages.
Also add disclaimer to replies (in-reply-to header set)	Adds the standard disclaimer to all outgoing email messages, which have been sent by the internal user in response to a received message.
Reprocess mails sent to reprocess@decrypt. reprocess	Allows you to perform the decryption process of a received email again.
Show message subject in logs	Enables the display of the subject line in the log files.

»Do not touch mails with the following text in subject« parameter

```
Standard: \[plain\]
```

Define a tag to prevent the cryptographic processing of an email. Paste this tag, including the square brackets in the subject line, so that this email will not be cryptographically processed by the ruleset. The ruleset can thus be »bypassed«. The backslashes inside the tag represent escape symbols. These should not be typed in by the user.

```
Example:

Subject: [plain] secure email encryption
```

Enable this parameter to give the user the opportunity to bypass the established ruleset.

»Add disclaimer to all outgoing mails« parameter

Use this setting, if you want to attach the standard disclaimers to all outgoing email messages.

»Also add disclaimer to replies (inreply-to header set)« parameter

Use this setting, if you want to attach the standard disclaimer to an email, which the internal user has replied to.

© 2014 SEPPmail AG

»Reprocess mails sent to reprocess@decrypt.reprocess« parameter

This setting applies to encrypted emails, that were sent to internal email recipients and could not be decrypted by the SEPPmail system. This case may occur, e.g. if the secure email system does not have, at the time of receipt, the required keying material of an email. Use this parameter to allow appropriate users to send emails, which could not be deciphered, to the address »reprocess@decrypt.reprocess«, to trigger the decryption process again using SEPPmail appliance.

»Show message subject in logs« parameter

Use this setting, if the subject line of an email should be displayed in the log files.

»Ruleset« section -> »User Creation« pane

Parameter	Description
Manual user creation: Only process outgoing mails from users with an account	Disables automatic creation of user accounts.
automatically create accounts for new users if user tries to sign / encrypt	Enables the automatic creation of user accounts, when trying to use the cryptographic functions.
automatically create accounts for all users	Enables the automatic creation of user accounts for all internal sender email addresses, from which emails are transported through SEPPmail.

»Manual user creation: Only process outgoing mails from users with an account« parameter

Enable this parameter, if you want to use the SEPPmail appliance only to allow those persons, who already have a user account on the appliance.

»automatically create accounts for new users if user tries to sign / encrypt« parameter

This parameter enables the automatic creation of new accounts. If this setting is active, internal email senders are automatically recorded as a user on the appliance. This is done, when the internal email sender tries to sign or encrypt an email.

»automatically create accounts for all users« parameter

This parameter enables the automatic creation of new accounts. If this setting is active, internal email senders are automatically recorded as user on the appliance.

© 2014 SEPPmail AG

»Ruleset« section -> »Encryption / Decryption« pane -> »Incoming Emails«

Parameter	Description
Add this text to message subject after decryption	Defines a tag to mark a successfully decrypted email
Set confidential flag after decryption	Sets the Outlook message option »confidential« after successful decryption
Reject mails if S/MIME decryption fails	Reject incoming S/MIME encrypted emails, which cannot be successfully decrypted

»Add this text to message subject after decryption« parameter

```
Standard: \[secure\]
```

You can define a tag to mark a successfully decrypted email. This is appended to the end of the subject line of a decrypted email. The backslash inside the tags represent escape symbols for the opening and closing square bracket. The inserted backslashes will be removed by SEPPmail.

```
Example:

Subject: Secure email encryption [secure]
```

»Set confidential flag after decryption« parameter

If an incoming email is decrypted by SEPPmail , then the Outlook »confidential« message option is automatically set in a forwarded internal email. When replying, this message option is retained and the outgoing email is also encrypted by SEPPmail.

»Reject mails if S/MIME decryption fails« parameter

Enable this parameter, if the incoming encrypted emails should be rejected, if the decryption fails.

»Ruleset« section -> »Encryption / Decryption« pane -> »Outgoing Emails«

Parameter	Description
Always encrypt mails with the following text in subject	Outgoing emails are encrypted, if the specified tag was inserted into the subject.
Always encrypt mails with Outlook "confidential" flag set	Outgoing emails are encrypted, if is Microsoft Outlook "confidential" message option is set.
Always use GINA technology for mails with the following text in subject	Outgoing emails are encrypted via GINA technology, if the specified tag was inserted into the subject.
Always use GINA technology for mails with Outlook "private" flag set	Outgoing emails are encrypted via GINA technology, if the Microsoft Outlook "Private" message option is set.

© 2014 SEPPmail AG

Parameter	Description
Create GINA users with empty password if the following text is in the subject	For newly generated GINA accounts, a blank password is set, when the specified tag was inserted into the subject.
Always use S/MIME or openPGP, if keys are available	Outgoing emails are automatically S/MIME or OpenPGP encrypted, if keying material of the recipient exists in the SEPPmail keystore.
Always use GINA encryption, if account exists and no S/MIME or openPGP key is known	Outgoing emails are automatically encrypted via GINA technology, , if the recipient's GINA user account exists and no keying material of the recipient is available in the SEPPmail key memory.
Do not encrypt outgoing mails with the following text in subject	Outgoing emails are NOT encrypted, if the specified tag was inserted into the subject.

»Always encrypt mails with the following text in subject« parameter

```
Standard: \[confidential\]
```

You can define a tag to initiate the encryption of outgoing email. Paste this tag, including the square brackets in the subject line, and SEPPmail sends this email encrypted. The appropriate encryption method is automatically selected by SEPPmail. The backslashes inside the tags represent escape symbols. These should not be typed by the user.

```
Example:

Subject: [confidential] secure email encryption
```

Order of encryption methods

1. S/MIME user encryption
2. PGP user encryption
3. S/MIME domain encryption
4. PGP domain encryption
5. Encryption as GINA message

The encryption methods are tried to be implemented in order. If no keying material of the recipient is found in SEPPmail key memory, the email will be sent via the ad hoc encryption as GINA message.

If the use of the GINA technology disabled, and an email cannot be otherwise encrypted, this email is rejected by SEPPmail and will not be sent. The sender will receive an email notification. It is used as the contents of the »bounce_noenc» template.

»Always encrypt mails with Outlook "confidential" flag set« parameter

Use this parameter, if emails in Microsoft Outlook should always be encrypted with the message

© 2014 SEPPmail AG

option »Confidential«. The procedure is analogous to the previous menu point.

»Always use secure webmail technology for mails with the following text in subject« parameter

```
Standard: \[priv\]
```

You can define a tag to initiate the encryption of outgoing email. Paste this tag, including the square brackets in the subject line, for SEPPmail to send this email encrypted. The encryption method to be used is the GINA enforced technology. The backslashes inside the tags represent escape symbols. These should not be typed by the user.

```
Example:

Subject: [priv] secure email encryption
```

»Always use secure webmail technology for mails with Outlook "private" flag set« parameter

Use this option if you emails should always be encrypted in Microsoft Outlook with the message option »Private«. The technology of the GINA is used as the enforced encryption method.

»Create Secure webmail users with empty password if the following text is in the subject« parameter

```
Standard: \[emptypw\]
```

You can define a tag for GINA to create user accounts with a blank password. Paste this tag including the square brackets in the subject line. The receivers of the GINA messages do not receive initialization password. They determine their personal passwords during the initial login within the GINA portal itself. The backslashes inside the tags represent escape symbol. These should not be typed by the user.

```
Example:

Subject: [emptypw] secure email encryption
```

»Always use S/MIME or OpenPGP if keys are available« parameter

Enable this parameter, to encrypt outgoing emails via S/MIME or OpenPGP, if appropriate keying material from the recipient exists in the SEPPmail keystore. The encryption is done only, when there is an active user account for the internal sender with an existing keying material of the recipient.

»Always use Webmail encryption if account exists« parameter

Enable this parameter always to send outgoing email as GINA message, if GINA user account already exists for the recipient. The use of GINA technology is enforced for all emails to the recipient.

»Do not encrypt outgoing mails with the following text in subject« parameter

```
Standard: \[noenc\]
```

© 2014 SEPPmail AG

You can define a tag to prevent encrypting an outgoing email. Paste this tag, including the square brackets in the subject line, so this email will not be cryptographically processed by the ruleset. The ruleset can thus be »bypassed«. The backslashes inside the tags represent escape symbols. These should not be typed by the user.

```
Example:

Subject: [noenc] secure email encryption
```

»Ruleset« section -> »Signing« pane -> »Incoming Emails«

Parameter	Description
Add this text to message subject if S/MIME signature check succeeds	Adds a status information in the subject line of the email, if the S/MIME signature verification was successfully performed.
remove signature if S/MIME signature check succeeds	Removes the S/MIME signature within the email, if the S/MIME signature verification was successfully performed.
Add this text to message subject if S/MIME signature fails	Adds a status information in the subject line of the email, if the S/MIME signature verification could NOT be successfully carried out.
remove signature if S/MIME signature check fails	Removes the S/MIME signature within the email, if the S/MIME signature verification could NOT be successfully carried out.

»Add this text to message subject if S/MIME signature check succeeds« parameter

```
Standard: \[signed\sOK\]
```

You can define a tag for an S/MIME signed email to highlight, that its signature was successfully verified. This tag is appended to the end of the subject line of a signed email. The backslashes inside the tags represent escape symbols for the opening and closing square bracket. The backslashes will be removed by SEPPmail. The S/MIME signature is tested against the root CA certificates in the SEPPmail certificate store (Menu »X.509 Root certificates«). When examining, only root CA certificates with the status of »trusted« is considered.

```
Example:

Subject: Secure email encryption [signed OK]
```

»remove signature if S/MIME signature check succeeds« parameter

Enable this parameter, if you want to remove the S/MIME signature of an email. This will only be executed, if the S/MIME signature could be successfully tested against a root CA in own Root CA store by SEPPmail. (See »X.509 Root Certificates« 169 menu)

»Add this text to message subject if S/MIME signature fails« parameter

```
Standard: \[signed\sINVALID\]
```

© 2014 SEPPmail AG

You can define a tag to mark, that a signature of an S/MIME signed email was NOT successfully validated. This tag is appended to the end of the subject line of a signed email. The backslashes inside the tags represent escape symbols for the opening and closing square bracket. The backslashes are removed when passing through SEPPmail. The S/MIME signature is tested against the root CA certificates in the SEPPmail certificate store (»X.509 Root certificates« menu). When examining, only root CA certificates with the status of »trusted« is considered.

```
Example:

Subject: Secure email encryption [signed INVALID]
```

»remove signature if S/MIME signature check fails« parameter

Enable this parameter, if you want to remove the S/MIME signature of an email. This will only be executed, if the S/MIME signature could not be successfully checked against a root CA in own Root CA store by SEPPmail. (See »X.509 Root Certificates« 169 menu)

»Ruleset« section -> »Signing« pane -> »Outgoing Emails«

Parameter	Description
S/MIME sign outgoing mails with the following text in subject	Outgoing emails are S/MIME signed, if the specified tag was inserted into the subject.
Sign all outgoing emails, if S/MIME certificate available	Outgoing emails are S/MIME signed, if there is a user account and an S/MIME certificate is available for the internal sender.
Do not S/MIME sign outgoing mails with the following text in subject	Outgoing emails are NOT S/MIME signed, if the specified tag was inserted into the subject.
S/MIME sign outgoing mails with domain key with the following text in subject	Outgoing emails are S/MIME signed, if the specified tag was inserted into the subject. Here, the S/MIME user certificate of the sender is not used, but the certificate specified by email of the defined user.

»S/MIME sign outgoing mails with the following text in subject« parameter

```
Standard: \[sign\]
```

You can define a tag to sign an outgoing email. Paste this tag to including the square brackets in the subject line. If outgoing emails are not signed by default, the user can initiate the signing of the current email. The backslashes inside the tags represent escape symbols. These should not be typed by the user.

```
Example:

Subject: [sign] secure email encryption
```

© 2014 SEPPmail AG

»Sign all outgoing emails, if S/MIME certificate available« parameter

Enable this parameter, if all outgoing emails to be signed by a corresponding S/MIME certificate for the sender are available.

»Do not S/MIME sign outgoing mails with the following text in subject« parameter

```
Standard: \[nosign\]
```

You can define a tag to NOT to sign an outgoing email. Paste this tag, including the square brackets in the subject line, and this email will not be cryptographically processed by the ruleset, if it would correspond any of the defined conditions. The ruleset can thus be »bypassed«. The backslashes inside the tags represent escape symbols. These should not be typed by the user.

```
Example:

Subject: [NoSign] secure email encryption
```

»S/MIME sign outgoing mails with domain key with the following text in subject« parameter

```
Standard: \[domainsign\]
```

You can define a tag to sign an outgoing email with a domain certificate of your organization. Paste this tag, including the square brackets in, the subject line. If outgoing emails are not signed by default, the user can initiate the signing of the current email. The backslashes inside the tags represent escape symbols. These should not be typed by the user.

```
Example:

Subject: [domain sign] secure email encryption
```

Other configuration parameters:

1. Using Certificate : to use the domain a certificate in a SEPPmail
2. Text before new FROM : text before the domain sender
3. Text after new FROM : text after the domain sender

»Ruleset« section -> »Key Generation« pane

Parameter	Description
automatically create openPGP keys for new users	automatic generation of OpenPGP user keys
automatically create S/MIME keys for new users	automatic generation of S/MIME user certificates
automatically buy ..... S/MIME keys for new users	setting to obtain S/MIME user certificates on the indicated CA connector

© 2014 SEPPmail AG

»automatically create openPGP keys for new users« parameter

This parameter causes automatic generation of OpenPGP keys for new users.

»automatically create S/MIME keys for new users« parameter

This parameter causes automatic generation of S/MIME certificates for new users.

»automatically buy SwissSign S/MIME keys for new users« parameter

This parameter is not visible by default. It is displayed as a function of the activated CA connectors. Enable this, to automatically obtain user certificates for new users of the respective CA connector.

The following CA-connectors on the »CA« menu are available:

1. S-TRUST : CA from Deutscher Sparkassen Verlag GmbH
2. none : CA connector is disabled
3. Signtrust : CA from Deutsche Post Signtrust and DMDA GmbH
4. SwissSign : CA from SwissSign AG (100%-owned subsidiary of Swiss Post)

»Ruleset« section -> »Protection Pack (Anti-SPAM / Anti-Virus)« pane

Parameter	Description
Check mails for viruses and send infected mails to (leave empty to reject infected mails)	Enables the virus scanner and sends infected messages to the specified email address.
Send notification to this email address if a virus was found	Sends a notification of virus detection to the specified email address.
Check incoming mails for spam and add the following text to the subject to identify spam	Enables verification of incoming SPAM emails and marks them after a successful SPAM testing.
Check incoming mails for spam and redirect spam to (leave empty to reject spam)	Enables SPAM testing and sends recognized as SPAM emails to the email address.

»Check mails for viruses and send infected mails to (leave empty to reject infected mails)« parameter

You can check incoming emails for viruses and forward upon detection of infection to the additionally specified email address with this parameter. The original recipient does not receive the infected email. If no email address is specified, corresponding emails will be deleted.

»Send notification to this email address if a virus was found« parameter

© 2014 SEPPmail AG

If a virus is found in an incoming email, a notice of that event will be sent to the email address specified here.

»Check incoming mails for spam and add the following text to the subject to identify spam« parameter

```
Default: [SPAM]
```

You can use this parameter to scan incoming emails for SPAM. If it is recognized as a SPAM email, the additionally defined tag is added to the end of the subject line to mark the email as SPAM.

Tag level: Here you define a threshold, above which an incoming email is classified and marked as SPAM. The lower this value, the more likely it is, that an email is detected as SPAM. At the same time, at low values a false detection increases the risk, that legitimate emails are detected as SPAM. A SPAM recognized and marked email will be sent to the original recipient.

»Check incoming mails for spam and redirect spam to (leave empty to reject spam)« parameter

With this parameter you can check incoming email for SPAM and forward one with a positive recognition to the email address, also specified here. The original recipient does not any more receive this email. If no email address is specified, corresponding emails will be deleted.

Spam level: Here you define a threshold, above which an incoming email is classified as SPAM and forwarded to the specified email address. If no email address is specified, corresponding emails will be rejected on receipt.

»Ruleset« section -> »Header tagging« pane

If the SEPPmail system is used along with other email processing systems reliant on inbound, outbound, encrypted and decrypted emails, will these receive a special mark, so that you can mark these by self defined »X-Header« map. An additional email processing system may replace these with »X-Header« set by SEPPmail to evaluate and react to it. An example for an additional email processing system, can be a Data Loss Prevention (DLP) system.

Parameter	Description
Set header X-..... to value ..... For all incoming mails	X-header and value for all by SEPPmail received emails, e.g. of internal or external received emails.
Set header X-..... to value ..... For all outgoing mails	X-header and value for all by SEPPmail sent emails, e.g. GINA messages, that are generated by GINA or status messages generated by SEPPmail.
Set header X-..... to value ..... For all mails that have been encrypted	X-header and value for all by SEPPmail encrypted emails

© 2014 SEPPmail AG

Parameter	Description
Set header X-..... to value ..... For all mails, that have been decrypted	X-header and value for all by SEPPmail decrypted emails

»Ruleset« section -> »Archiving« pane

Parameter	Description
Send a copy of ALL emails to the following Address	All through SEPPmail transported emails are sent to the specified email address in copy.

»Ruleset« section -> »Custom Commands« pane

Parameter	Description
Custom commands for incoming Email	Ruleset commands for processing of incoming messages
Custom commands for outgoing email	Ruleset commands for processing of outbound messages
Custom commands for User Creation	Ruleset commands for creating user accounts

These additional user-defined Ruleset commands are in each case inserted at the beginning of the corresponding section in the Ruleset-source code and processed first.

»Custom commands for incoming email« parameter

Use this pane to enable additional user-defined Ruleset commands for processing of incoming messages.

»Custom commands for outgoing email« parameter

Use this pane to enable additional user-defined Ruleset commands for processing of outbound messages.

»Custom commands for User Creation« parameter

Use this pane to enable additional user-defined Ruleset commands for creating user accounts.

Example:

```
if (authenticated()) {
} else {
   createaccount('@CREATEGPGKEYS@');
   log(1, 'user account generated');
}
$?$
```

© 2014 SEPPmail AG

»Ruleset« section -> »Advanced Options« pane

Parameter	Description
Re-inject mails to sending mailserver (use with care!)	Processed emails will be sent back to the the delivering email server
Run in queueless mode (use with care!)	Enables the Queueless mode for the processing of email
Completely disable GINA technology	Disables the GINA subsystem
Completely disable user-based S/MIME and openPGP	Disables the user-based S/MIME and OpenPGP encryption and decryption

»Re-inject mails to sending mailserver (use with care!)« parameter

With this setting, all emails will be returned after processing to the server from which they were sent to SEPPmail (e.g. central mail hub).

»Run in queueless mode (use with care!)« parameter

This setting causes emails to individual recipients during processing to not to be »cached«. Instead, the connection of the consigned email will only be acknowledged, if the processed email has been forwarded to the next email server, and this outgoing connection has been acknowledged. If the acceptance for some recipients is not acknowledged, when sending to multiple recipients, these emails are briefly located on the appliance, until it is acknowledged by the receiving email server.

»Completely disable secure webmail technology« parameter

With this option, you can disable the GINA technology center. This may be necessary, if SEPPmail is not reachable from the outside or the GINA technology is not needed.

»Completely disable user-based S/MIME and openPGP« parameter

With this parameter you can centrally disable the user encryption for S/MIME and OpenPGP. This may be necessary if only want to exclusively use the GINA technology or domain encryption.

»Ruleset« section -> »Advanced Options« pane -> »Remote GINA Relay«

Parameter	Description
Use remote GINA server, reachable under the following email address	Email address of the remote GINA servers
This is a remote GINA server	Configuration parameters, if you are using SEPPmail as remote GINA relay

© 2014 SEPPmail AG

To use the GINA technology, it is necessary that SEPPmail system can be reached from the Internet. If this is not possible, you cannot use the GINA technology. To avoid this situation, you can use an external SEPPmail system as a remote GINA relay.

»Use remote GINA server, reachable under the following email address« parameter

The communication between the internal SEPPmail and the SEPPmail which is used as a remote GINArelay , is done via email. Enter the email address to be used for communication.

SEPPmail provides in this case no GINA functionality, but forwards outgoing emails via GINA technology to be sent further to the remote GINA relay. In this case, enter no values for the parameters under »This is a remote Webmail server«.

»This is a remote GINA server« parameter

Use SEPPmail as a remote GINA relay, then enter the values for the following parameters. Apply for the »Use remote GINA server, reachable under the following email address« parameter with no value.

Relay for domain
Email domain(s) of the GINA sender. For the specified email domain(s) this system provides the GINA function after being ready externally. This system produces GINA emails and provides the portal for external users for decryption ready.

Relay email address
Email address of the remote GINA Relay. Under this email address, this system is accessible as a remote GINA relay.

Relay domain key fingerprint
Fingerprint of the domain key, which is used by this relay server.

6.6.7 Viewing and loading rulesets

»Mail Processing« menu -> »SMTP Ruleset« section

Parameter	Description
Display	Displays the current ruleset.
Upload	Enables uploading of a custom ruleset.

© 2014 SEPPmail AG

6.7 "SSL" menu item

Select the »SSL« menu item to manage the SSL device certificate (Secure Sockets Layer) of the SEPPmail appliance.

Following procedures are described in the chapters hereafter:

Creating self SSL device certificate 103
Requesting SSL device certificate from a public CA 105
Using existing SSL Device Certificate 106
Backing up SSL device Certificate 106

6.7.1 Creating self SSL device certificate

»SSL« -> menu »Request a new Certificate...« button

SEPPmail makes it possible to create own SSL device certificates via the configuration interface. For a test installation, it is not absolutely necessary to obtain a paid SSL device certificate. The certificate can be automatically generated and signed on the SEPPmail appliance.

Fill in the fields as follows (the italic fields must be filled in):

»Issue To« section

Parameter	Description
Name or IP (CN)	IP address or host name at which SEPPmail is accessible from the Internet. A self-signed certificate here must match with the specified values of the name in the URL under which the SEPPmail is addressed. **Example:** If SEPPmail should be addressed at the URL **»https://securewebmail.example.tld«**, it is the **»Name or IP (CN)«** field, that should specify the **»securewebmail.example.tld«** host name.
Email	A valid email address within the company, at which a competent person can be reached.
Org. Unit (OU)	Name of competent organizational unit (optional).
Organization (O)	Name of the organization (optional).
Locality (L)	Place, where the organization has its headquarters (optional).
State (ST)	Canton/state or province where the organization has its headquarters (optional).

© 2014 SEPPmail AG

Parameter	Description
Country (C)	Country, in which the organization has its headquarters.

»Attributes« section

Parameter	Description
Key size (bits)	Key length in bits Possible values: 1024 or 2048 Select always the value »2048« for the key length. Shorter keys are no longer considered sufficiently secure.
Signature	For this parameter, the following values are available: »Create Certificate signing request« — Creates a certificate request (CSR) to sign a public CA. »Create self-signed certificate« — Creates a self-signed SSL device certificate. Select »Create self-signed certificate« in order to create a self-generated and self-signed SSL device certificate.

To execute the creation of the SSL certificate, click on the »Create Request« button. You will then receive a confirmation with the certificate details.

It is also possible to create wildcard SSL certificate. Wildcard certificates are valid not only for a dedicated host, but can be used for multiple hosts in a domain.

Example: an SSL certificate with the name ginatest.testdomain.net can only be used for this host. Otherwise, a certificate error message is displayed in the web browser. You can use a Wildcard SSL Certificate on any of the hosts in a domain, e.g. ginatest.testdomain.net, webmail.testdomain.net or secmail.testdomain.net.

To create a wildcard SSL certificate, enter the host name as follows: *. Customerdomain.tld.

After entering the information, you will receive a confirmation with the certificate details. This includes the values of the following information, that you have specified:

1. the serial number of the certificate (Serial No.)

© 2014 SEPPmail AG

2. the period of validity (Validity)
3. the Fingerprint (SHA1 Fingerprint)

Please note that a restart of the SEPPmail appliance is required to enable the new SSL device certificate. You can execute the reboot by clicking on the »Administration« menu item the »Reboot« button and then confirm the displayed security code.

6.7.2 Requesting SSL device certificate from a public CA

»SSL« menu -> »Request an new Certificate...« button

Proceed as follows:

1. Perform the same steps than in the chapter Create yourself SSL device certificate 103, but select for the »Signature« parameter the value »Create Certificate signing request«, to create a certificate request (CSR). To create the certificate request, select the »Create Request« button.

2. Select the button »Download and Import signed Certificate...«.

> **Note:**
>
> In case the upper area of the menu with the yellow background information displays **»Remember to import the signed certificate.«**, a certificate request has been previously created.

3. Copy the text in the »Request« section and submit it to the certification authority, from which you want to request the SSL device certificate. You should once more save this CSR locally in a text file for safety. With many certification bodies, you can paste the certificate request (CSR) in the web portal for the designation of the SSL device certificate.

4. Once you have received your SSL device certificate from the certificate authority, select in the »SSL« menu the »Download and Import signed Certificate...« button

5. Paste the certificate into the »Import Certificate« section and then select the »Import Certificate« button. The process of creating a new SSL certificate for the device SEPPmail appliance is now complete. To activate the new SSL.Device certificate, please reboot the SEPPmail system.

> **Note:**
>
> Add the newly created own SSL device certificate together with the required additional certificates for one or more intermediate CA certificates, and the certificate of the root CA itself in the order shown. Make sure, that the order, in which the elements of the certificate are inserted, is correct. In case of error, you cannot use the SSL device certificate. There may also be problems in accessing the configuration interface. In this case, you can access the configuration interface using the HTTP protocol on port TCP/8080. (http://<Appliance>:8080)

© 2014 SEPPmail AG

Sequence for the insertion of the elements of the certificate:

1. Public key of own SSL device certificate
2. Public key from one or more intermediate CA certificates
3. Public key of the root CA

6.7.3 Using existing SSL Device Certificate

»SSL« menu -> »Request a new Certificate...« button

»Upload existing key« section

Parameter	Description
X.509 Key	Insert the private key of the certificate.
X.509 Certificate	Insert the public key of the certificate.

»X.509 Key« parameter

Insert in this field the private key of the certificate. If the private key is protected by a password, this must first be removed.

Parameter »X.509 Certificate (and optional intermediate certificates)«

Insert in this field the public key of the certificate. In addition to its own public key, add here also a further optional dual use certificate (Intermediate Certificates) and the public key of the root CA certificate. This yields a certificate chain (Chain), which the SEPPmail web server passes to the user's web browser, and which are used to verify the SSL device certificate.

Order for the insertion of the elements of the certificate:

1. Public key of own SSL certificate device
2. Public key of one or more intermediate CA certificates
3. Public key of the root CA

Complete the process in both cases, by clicking on the "Create Request" button.

6.7.4 Backing up SSL device Certificate

»SSL« -> menu »Backup Certificate« button

Back up the certificate by clicking on the »Backup Certificate« button. You can save the currently installed SSL device certificate (public and private key) as a file on the local hard drive. The certificate file is in PEM format and has the name »cert.pem«.

Example:

© 2014 SEPPmail AG

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDqLer/5Tp0j/+v
.
.
.
KHp36xzcsUNklzcPW89MWdUccLKmMf+KTDQBaJqrHplhSgtkKLh+MdyzTCEgkldT
VFbcif6/k5dNnDxz/wCZSzQ=
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIFIjCCBAqgAwIBAgIJALbNmR60XAsAMA0GCSqGSIb3DQEBBQUAMIGmMRcwFQYD
.
.
.
7ej1ce+YN2vIn2mYMFtn0D+yCxP9mPLsAGEdO6EaY/IPRaVNJUI8XYmJSicyOzIY
PCqvmnfimMsxA3u0rID+ein0SwbR+g==
-----END CERTIFICATE-----
```

© 2014 SEPPmail AG

6.8 "CA" menu item

Select the »CA« menu item to manage your own Certificate Authority (CA) on the SEPPmail appliance.

Following procedures are described in the chapters hereafter:

Managing internal CA settings 108
Setting up CA certificate 109
Securing CA certificate 109
SwissSign 110
Signtrust 110
S-Trust 109

6.8.1 Managing internal CA settings

»CA«

»Certificate Revocation List« section

»Download Certificate Revocation List (CRL)« parameter

Click on the »Create and Download CRL« button to download and view the CRL. The CRL file can be downloaded at the following address directly from the SEPPmail web server:

https://<IP-Adresse-SEPPmail>/certs.crl

»Internal CA Settings« section

Adjust the settings of the internal CA according to the details of your organization. The values given are taken into account when generating certificates by the local SEPPmail CA.

»Static Subject Part« parameter

C : Country in which the organization is based
OU : Name of competent organizational unit
O : Name of the organization

»Validity in days« parameter

Validity of the CA certificate in days

»Extension settings« parameter -> »Additional parameters« pane

name : name of the parameter
value : corresponding value

Example:

SEPPmailsupports as a default feature the exhibiting and providing a CRL as a file for external download. To be effective, it is necessary to specify the revocation list distribution points in the certificate.

Add to this the following additional parameters:

© 2014 SEPPmail AG

```
name      : crlDistributionPoints
value     : URI:https://<Hostname SEPPmail>/certs.crl
```

»External CA« section

Activate one of the existing CA-connectors to automatically obtain user certificates on the managed PKI of an external CA. In a managed PKI, it is the interface to a certificate provider, which enables automated retrieval of certificates. For this purpose there is typically a contractual agreement with the selected certificate provider required. The following certificate provider Signtrust offers this at a very easy-to-use on line application.

You can reach the Signtrust online application under this link: Signtrust on line application

The following CA-connectors are available in the »CA« menu:

1. S-TRUST : CA from Deutscher Sparkassen Verlag GmbH
2. none : CA connector is disabled
3. Signtrust : CA from Deutsche Post Signtrust and DMDA GmbH
4. SwissSign : CA from SwissSign AG (100%-owned subsidiary of Swiss Post)

6.8.2 Setting up CA certificate

»CA« menu

To generate a CA certificate, click on the »Request a new Certificate...« button. During the certificate creation, follow to the steps described analogously in the chapter Setting up SSL certificate 103.

6.8.3 Securing CA certificate

»CA« menu

Perform the backup by clicking the »Download Certificate« and »Download Key« buttons.

Button	Description
»Download Certificate«	Secure the public part (public key) of the CA certificate.
»Download Key«	Secure the private part (private key) of the CA certificate.

6.8.4 Setting up a connection to the external CA S-Trust

»CA« menu

To set up the connection to the external certificate provider S-Trust, click on the »Save« button in the configuration interface. Click to »S-Trust connector...« button to edit the settings for the connection of S-Trust MPKI.

If you do not already have set up CA connector, choose a CA connector from S-Trust <% OEM CA3%

© 2014 SEPPmail AG

> and save this setting. Now you can configure the previously selected CA connector.

You will receive all required data for the configuration from the S-Trust CA.

6.8.5 Setting up a connection to the external CA Signtrust

»CA« menu

To set up the connection to the external certificate providers Signtrust, click in the configuration interface on the »Save« button. Click on the »Signtrust connector...« button to edit the settings for the integration of Signtrust MPKI.

If you do not already have set up any CA connector, choose a CA connector from Signtrust and save this setting. Now you can configure the previously selected CA connector.

You get all data required for the configuration from the Signtrust CA.

Parameter	Description
Certificate Request Sender Email	Email address that is used as the sender for the assignment of certificates.
Class 3 certificate	Selection of Class 3 certificates for personal identification of the administrator.
Password	Password for the Class 3 certificate of the administrator.

Note:

Please note that all from SEPPmail to the CA outbound emails and all from the CA returned emails are not changed, retained or deleted by an upstream SPAM filter. Define for that purpose within your use SPAM filter, the appropriate exceptions for the listed Parameter Certificate Request Sender Email Address and for the email used by the CA as the sender email stcertreq@support.signtrust.de.

To use the Signtrust CA connector, you can use the following online request.

The reference of user certificates via the Signtrust CA connector is done in the user account »Users« menu.

6.8.6 Setting up a connection to the external CA SwissSign

»CA« menu

To set up the connection to external certificate provider Signtrust, click on the »Save« button in the configuration interface. Click on the »Signtrust connector...« button, to edit the settings for the integration of Signtrust MPKI.

If you do not already have set up any CA connector, choose a CA connector from Signtrust and save this setting. Now you can configure the previously selected CA Connector.

© 2014 SEPPmail AG

You have the choice between Silver light certificates or Default certificates. To use Silver light certificates, no further information is required.

You will receive all required data for the configuration from the S-Trust CA.

© 2014 SEPPmail AG

6.9 "Administration" menu item

Select the »Administration« menu item to manage administrative tasks of the SEPPmail appliance.

Following procedures are described in the chapters hereafter:

Registering the appliance 112
Importing license file 112
Checking the appliance for available updates 113
Backing up and restoring settings of the appliance 114
Rebooting or shutting down the appliance 115
Resetting the appliance to the factory settings 116
Importing existing user or key 116
Establishing inbound remote support connection 117

6.9.1 Registering SEPPmail appliance

»Administration« menu -> »License and Registration« section

A registration of the SEPPmail system is required in order to obtain a permanent license.

Click on the »Register this device...« button and you will get a registration screen. Fill in the fields in the registration window with your details. Type in your customer information in the upper half and your customer information in the lower half of the window. Complete the entries by clicking the »Send« button.

If the »Registration successful« message appears, you have successfully completed the registration process.

Now a license for your system will be issued by SEPPmail for this installation. The import of the license at SEPPmail is done automatically through an online connection to the license server.

For registration and license terms, it is necessary that SEPPmail can establish an online connection to the Internet on destination port TCP/22 (SSH). If this is not possible, then the registration i.e. the license subscription fails.

6.9.2 Importing license file

»Administration« menu -> »License and Registration« section

The licensing of the SEPPmail appliance appears automatically after a short time, when you register the appliance (see chapter Register Appliance 112).

To manually record a license file, click on the »Import License File...« button. Click the »Browse«, button to select the license file you want to import.

You can view the current license information in the »Home« menu.

© 2014 SEPPmail AG

The use of the license files is no longer supported for new installations. For new installations, the licensing takes place exclusively via the online licensing.

6.9.3 Checking appliance for available updates

»Administration« menu -> »Update« section

To get your SEPPmail appliance updated to the latest software version, various options are available in the configuration interface.

Buttons	Description
Check for Update	Checks online for new updates and shows a release note.
Fetch Update	Downloads an existing update and installs it automatically.
Prefetch (reboot manually)	Downloads an existing update, but does not install it. The installation is done only after the next reboot.

»Check for Update« button

Click the »Check for Update« button to search online for available software updates for SEPPmail. If an update is available, this will be displayed. In addition, a release note is displayed.

»Fetch Update« button

Click on the »Fetch Update« button to install an existing update. This process can be time consuming, if the delivered system still contains an older firmware and therefore several updates must be performed. A system reboot is required after each update.

Repeat this step until no more available updates appear. The system optimizes this update process, so that no update needs to be installed for each intermediate version, but only for updates that change the data structure.

»Prefetch (reboot manually)« button

For customers with a network infrastructure and when the updates can only be done within purpose provided for this period (maintenance window), a software update can be downloaded in advance. You can perform the actual update in the maintenance period by restarting the SEPPmail system.

Use the »Prefetch (reboot manually)« button to start downloading the update. After the download, a status message is displayed below the buttons. After a reboot, the previously downloaded update will be automatically installed.

General Notes

It may be in certain circumstances happen, that you will not get any feedback for a long time. If this is

© 2014 SEPPmail AG

the case, refresh the view by clicking on the »System Administration« link above the buttons. As long as you have not logged out, the update is not completed yet.

The SEPPmail appliance must check for updates at each performed restart and you have to login again. Perform this step by yourself, if necessary, if the system for a long time gives no feedback, and no login screen is displayed. Check again after rebooting, if further updates are available.

If you receive the message »You already have the latest version installed« your SEPPmail appliance has the latest software version. If in the future more updates become available, they are automatically displayed after restarting in the »Home« menu and the »Administration« menu.

If you want to access the »Administration« menu and this process takes a very long or longer than usual, then SEPPmail cannot check for new updates on line. If necessary, check your firewall configuration. The »Administration« menu is displayed anyway after a slightly longer wait time.

6.9.4 Backup and restore settings of the appliance

»Administration« menu -> »Backup« section

The services to back up or restore the settings of the SEPPmail appliance are available in the configuration interface with various options.

Important note:

A system backup contains all configuration data, except the following:

1. the local SSL Device Certificate
2. the local root CA certificate
3. the local cluster identifier

Make sure that the exceptions referred for separate backup manually by the system backup are secured. In case of failure, you can only restore the data contained in the system backup and which you have manually backed up in addition to the system backup.

The following transaction data are also not included in the system backup:

1. the local log files
2. the local system statistics
3. the local LFM store
4. the local email queue

Buttons	Description
Backup: Download	Manually downloading a system backup
Backup: Changing Password	Changing the Backup Password
Restore: Importing Backup File...	Manually restoring a System Backup

© 2014 SEPPmail AG

Buttons	Description
Restore: Importing ldif...	Manually restoring an LDIF file

General information to the backup

To save the current status of your SEPPmail appliance, you must first specify a backup password. This is required when restoring a backup.

»Download« button

To perform the backup, click the »Download« button. You obtain an encrypted file to save locally. For encryption, the specified password is being used.

»Change Password« button

Before creating the first backup, it is required that you assign a password to secure the backup files. This password is required to restore the backup file in case of failure. To change the password for future backups, click the »Change Password« button.

Attention, the change affects only future backups! Backup files from the past are still protected with the corresponding previously set password.

»Import Backup File« button

To import a backup file and thus restore settings of the appliance, click on the »Import Backup File...« button. To carry out the restore, select the subsequent dialog from the backup file, and enter the corresponding password.

6.9.5 Rebooting or shutting down the appliance

»Administration« menu -> »System« section

Button	Description
Reboot...	Rebooting the system
Shut down...	Shutting down and turning off the system

To prevent an accidental reboot or an accidental shutdown, these operations must be confirmed with a security code. The security code is generated automatically and displayed and must be entered in the »Security code« field.

```
Example:

Please enter the ivahkagh security code in the field below.
```

© 2014 SEPPmail AG

```
Here, the »ivahkagh« string is the Security Code.
```

This must be entered in the »Security code« field. Then click on the »Reboot system now...« button, to perform a restart. Proceed analogously for the system shut down.

6.9.6 Reseting the appliance to factory settings

»Administration« menu -> »Database and System Settings« section

To reset the system to factory settings, click on the »Perform factory reset...« button. To prevent an undesired reset of the system, this procedure must be confirmed with a security code. The security code is generated automatically and displayed, and you must enter it in the »Security code« field in reverse order (back to front).

After correctly entering the security code and by clicking the »Factory reset!« button, the confirmation message »Factory reset in progress. The device will automatically switch off after finishing« will appear. Once the process is complete, SEPPmail is automatically turned off.

To ensure that all data stored on the system is safely deleted, you have the option, by activating the »Secure Overwrite (Partitions will be overwritten ten times with random data, might take very long)« parameter, to override the areas of data memory 10 times with random data. This process takes a long time, but offers a higher level of security against unauthorized restore of deleted data.

6.9.7 Import existing user or key

»Administration« menu -> »Import« section

Button	Description
Import Users (CSV)	Import users from a CSV file
Import GINA Users (CSV)	Importing of GINA users from a CSV file
Import openPGP secret keys	Importing OpenPGP keys
Import S/MIME keys	Importing S/MIME key pairs
Import S/MIME certificates	Importing S/MIME public keys

"Import Users (CSV): import" button

> You can import user accounts by clicking on the »Import« button, next to »Import Users (CSV)«. The file containing user information must be in CSV (Comma Separated Values) format and have the following syntax: USERID;NAME;EMAIL;PASSWORD. The »PASSWORD« field is optional. The imported users will be displayed in the »Users« menu.

»Import GINA Users (CSV): Import« button

© 2014 SEPPmail AG

To import GINAusers, click on the »Import« button, next to »Import GINA Users (CSV)«. The file containing user information must be in CSV format and have the following syntax: EMAIL; PASSWORD. The imported users appear on the »GINA accounts« menu.

»Import openPGP secret keys« button

You can read in existing openPGP key pairs by clicking on the »Import openPGP secret keys« button. You can import the key in a file or in text format. In addition, you must enter the pass phrase of the respective key. If you want to import a larger number of OpenPGP keys at once, these keys must be combined into a key file. When importing the OpenPGP key pairs, a user account is created for each key pair. The appropriate OpenPGP key pair is automatically assigned for each user account.

»Import S/MIME keys« button

You can read in existing S/MIME certificates (key pairs) by clicking on the »Import S/MIME keys« button. The certificates must be as files in PKCS#12 format. To import a larger number of S/MIME certificates at once (bulk), you can combine them into a ZIP archive. This ZIP archive must not contain any directory structure and must not be secured by a password. By importing S/MIME certificates (key pairs) will create a user account for each key pair. The appropriate S/MIME key pair is automatically assigned for each user account.

»Import S/MIME certificates« button

You can read in existing S/MIME public keys by clicking on the »Import S/MIME certificates« button. The imported certificates are stored in the proper certificate store of SEPPmail. You find the read in S/MIME public keys in the »X.509 Certificates« menu.

6.9.8 Establishing Outgoing Support Connection

»Administration« -> menu »Establish Support Connection« section

The »Establish Support Connection« button opens a connection to the manufacturer. Use this function only according to instructions from the manufacturer. For the connection to be established, there must be an open connection to the Internet from the SEPPmail appliance in your firewall i.e. your router port TCP/22 (SSH).

To establish an incoming support connection, click in the configuration interface on the »Administration« menu item and then click the »Connect« button.

© 2014 SEPPmail AG

6.10 "Cluster" menu item

This chapter describes the basic operation and administration of the SEPPmail cluster. You will learn, which cluster modes are supported by SEPPmail and how to set them up in the configuration interface.

General information about the cluster modes 118
High Availability Cluster 118
Load Balancing Cluster 121
Geo Cluster (»MultiSite System«) 127
Frontend-Backend Cluster 128
Setting up a cluster configuration 129

6.10.1 General

There are different types of cluster operations, which are supported by SEPPmail.

A cluster refers to a computer network of several interconnected computer systems. These networked computer systems are physically separate, but are logically considered a single unit. It is thus possible, that a cluster can be addressed as a single logical system, but actually consists of several physical systems.

For the use of a cluster, there are several objectives, which indeed, differ by usage. For a cluster of several SEPPmail systems, there are the following 4 modes::

1. High Availability Cluster for fail safety (Failover)
2. Load Balancing Cluster for load distribution
   - Distribution of incoming and outgoing mail flow on each cluster member system
   - Use of an external load balancer to distribute the emails to different cluster member systems (depending on configuration)
   - Load distribution based on the Round Robin DNS method (http://en.wikipedia.org/wiki/Round-robin_DNS)
3. Geo cluster to replicate configuration databases at geographically from each other distant systems
4. Frontend-Backend Cluster

In the following chapters, each of the four operating modes are described in detail.

6.10.2 High Availability Cluster

The reliability of the SEPPmail system can be increased by the creation of a cluster.

The SEPPmail system has an integrated cluster function based on the CARP protocol (http://en.wikipedia.org/wiki/Common_Address_Redundancy_Protocol).

In order to form a cluster, at least two SEPPmail systems are required to monitor each other. If a system fails and no longer replies to these monitoring requests, the second system takes over its function. If the failed system becomes available again i.e. it again responds to the monitoring requests, it assumes its original task.

© 2014 SEPPmail AG

This feature can be mapped up to 9 SEPPmail systems, allowing you to achieve a very high level of reliability.

The high availability cluster systems can be mapped on hardware basis and on the basis of virtualization with VMware ESX with SEPPmail systems. Mixed operation with systems based on the hardware and virtualized systems is also possible.

How does the high-availability cluster work?

In this method, a cluster, one or more virtual IP address (es) are associated with different priorities. Each cluster member system has, independently of the assigned virtual cluster IP address, in each case its own unique IP address. Each cluster member system can be explicitly addressed on this own unique IP address.

Example:
In the following figure, the virtual cluster IP address of the cluster is 10.10.0.1. The cluster member systems have in our example, the IP address 10.10.0.9 and 10.10.0.10.

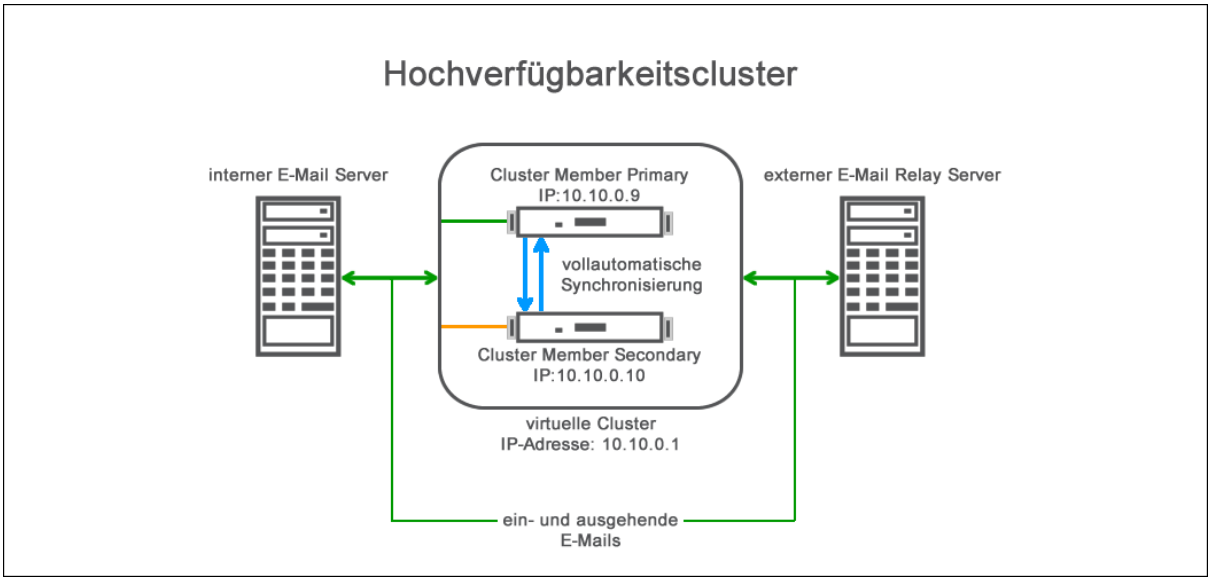


Figure 1 - Schematic representation of a high-availability cluster

The cluster itself will be addressed by other systems, e.g. an internal email server or an upstream email relay server (gateway) via the established virtual IP address(es). In the example above, this is the IP address 10.10.0.1.

If the cluster itself is addressed by its cluster IP address, then it always responds the cluster member system with the highest priority on the addressed virtual cluster IP address. All other cluster member systems with lower priority do not respond when the virtual cluster IP address is addressed and a cluster member system with a higher priority is available.

In case of failure, if a cluster member system fails with higher priority, which normally responds to the addressed virtual cluster IP address, then it automatically takes over a cluster member system with the next lower priority virtual cluster IP address, including the function of the failed cluster member system.

The priorities are organized in the following order:

© 2014 SEPPmail AG

1. Primary
2. Secondary
3. Backup

Setting the priority of each cluster member system, follow trough the steps in the »System« menu.

© 2014 SEPPmail AG

6.10.3 Load Balancing Cluster

A cluster can also be used to increase the email throughput. For this, there are the following options:

1. Distribution of incoming and outgoing email data flow to each cluster member system 121
2. Use of an external load balancer to distribute the emails to different cluster member systems (depending on configuration) 122
3. Load distribution based on the DNS Round-Robin method 123 (http://en.wikipedia.org/wiki/Round-robin_DNS)

Use with redundant external and internal MTAs (Mail Transport Agent) 125

The failover behavior of the cluster is not changed by these configurations.

Distribution of incoming and outgoing email data flow to each cluster member system

The allocation of the incoming and outgoing the email data stream, as mentioned above, takes place in three different ways. In figure 1, incoming and outgoing emails are sent through a static configuration each being connected to a separate virtual IP address. There are 2 SEPPmail systems with different priority to each of two virtual IP addresses (alias IP addresses) to respond. In each case, one system receives all incoming emails and another system receives all outgoing emails. By setting up two virtual IP addresses, the two SEPPmail systems can be addressed separately via a dedicated virtual IP address.

In figure 1, this is logically mapped. Physically, there are just two SEPPmail systems.

What happens in detail:

Each SEPPmail system has its own completely separate IP address, that can be accessed by only this system, e.g. to configure settings that are not synchronized in the cluster.

In figure 1, these are the IP addresses 10.10.0.9 and 10.10.0.10.

In addition, there are two virtual IP addresses to combine the two SEPPmail systems logically to one group. In figure 1, these virtual IP addresses (groups) are shown separated by different colors.

The virtual IP address 10.10.0.1, shown here in green, is addressed for all outgoing emails from the internal email server i.e. outgoing emails are sent by internal mail server to this virtual IP address.

The virtual IP address 10.10.0.2, shown here in orange, is addressable for all incoming emails from the external email server, or an upstream email relay (e.g. firewall), i.e. the incoming email messages are sent from the external or upstream systems to this virtual IP address.

Under a virtual IP address, the two physical SEPPmail systems are now grouped logically together. Basically both systems respond, if the virtual IP address is accessed. But this is not always useful, since we want always use one system for all incoming emails and the other system for all outgoing emails. To achieve this, the order in which the individual systems respond must be fixed in a specified hierarchy, if one of the virtual IP addresses is addressed.

In figure 1, shown in green, you will see the virtual IP address 10.10.0.1 for all outgoing emails. Here, the cluster member system is configured with the IP address 10.10.0.9 as primary and

© 2014 SEPPmail AG

always reacts as first system, when the virtual IP address 10.10.0.1 is addressed. The cluster member system with the IP address 10.10.0.10 is configured as secondary and responds only, if the primary cluster member is unavailable.

In Figure 1 shown in orange, you see the virtual IP address 10.10.0.2 for all incoming emails. Here, the cluster member system is configured with the IP address 10.10.0.10 as primary (as opposed to its previous appearance) and always reacts as the first system, when the virtual IP address 10.10.0.2 is addressed. The cluster member system with the IP address 10.10.0.9 is set as secondary and responds only, if the primary cluster member is unavailable.

Summary:

Each individual SEPPmail system can be accessed through two different virtual IP addresses and responds with different priorities even once as primary and once as secondary. Thus, the operation, in case of failure of a cluster member system, is still possible. The remaining cluster member system then takes over the work of the system, that is no longer available and will process all incoming and outgoing emails.

For the use of Enhanced Secure Webmail, a virtual cluster IP address 10.10.0.1. can be addressed. Depending on the cluster member priorities, the cluster member system will respond with the IP address 10.10.0.9, as this is set up with the »Primary« priority, in the example of figure 1. If this system is not available, the cluster member system will respond with the IP address 10.10.0.10, as this is set up with the »Secondary« priority.

The Setting up of virtual IP addresses and assigning priorities is performed in accordance with steps in the »System« menu.

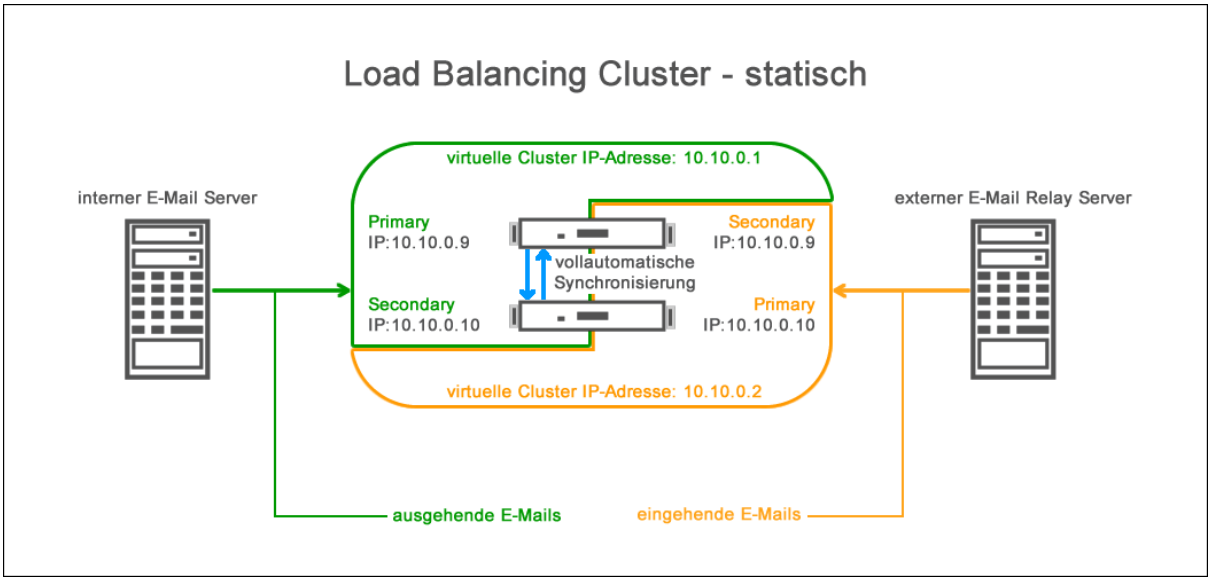


Figure 1 - Schematic representation of the static allocation for incoming and outgoing emails

Use of an external load balancer to distribute the emails to different cluster member systems
Figure 2 shows, how incoming and outgoing emails are sent by an external load balancer dynamically to the cluster member systems. Each cluster member system thus receives both incoming and outgoing emails. If a cluster member system is unavailable, the load balancer is responsible to recognize this, and reacts accordingly. Figure 2 shows a logical representation of the scenario.

What happens in detail:

© 2014 SEPPmail AG

The cluster functionality of SEPPmail is used in this scenario only for the synchronization of configuration between the cluster member systems. The decision, as to which system it responds for incoming and outgoing emails, is made by the upstream load balancer. This distributes, depending on configuration and load situation, the emails optionally to a cluster member system. Here, the cluster member system is not addressed via a virtual IP address, but by its own separate IP address.

Each SEPPmail system has its own completely separate IP address, that can be accessed by only this system, e.g. to configure settings, that are not synchronized in the cluster.

In figure 2, these are the IP addresses 10.10.0.9 and 10.10.0.10.

The essential difference from Figure 1 is, that in this case, no virtual IP address is accessed. To distribute outgoing emails, the load balancer will distribute these, on the internal email server, selectively to the cluster member systems with the IP addresses 10.10.0.9 and 10.10.0.10.

Summary:

When using an external load balancer, the SEPPmail cluster member systems are contacted directly by the Load Balancer. If a cluster member system fails, the load balancer is responsible to identify this and to send the incoming or outgoing email messages to the remaining system.

For the use of Enhanced Secure Webmail, the virtual cluster IP address can still be addressed. Depending on the cluster member priorities, the cluster member system will respond with the IP address 10.10.0.9, as this is set up with the »Primary« priority. If this system is not available, the cluster member system will respond with the IP address 10.10.0.10, as this is set up with the »Secondary« priority.

The setting up of virtual IP addresses and assigning priorities is performed in accordance with steps in the »System« menu.

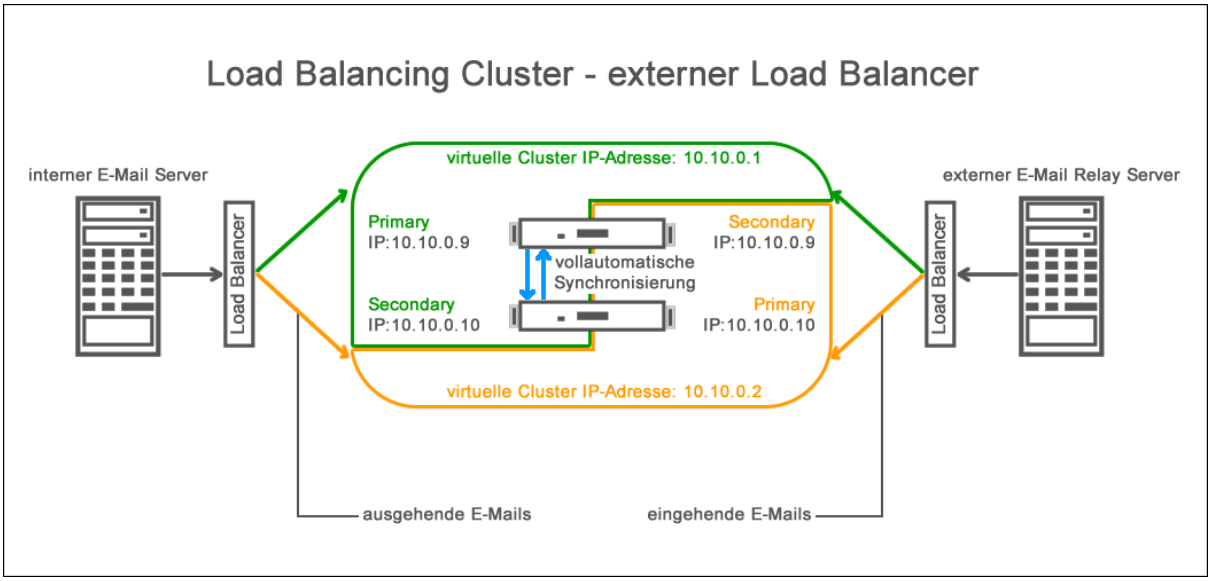


Figure 2 - Schematic representation of the dynamic allocation for incoming and outgoing emails through an external load balancer

Load balancing based on the DNS Round-Robin method

© 2014 SEPPmail AG

For a detailed description of this feature, see the following article: http://en.wikipedia.org/wiki/Round-robin_DNS

In the configuration of the internal and external email server, a virtual cluster IP address for email transmissions will no longer be specified, but in each case, a host name, e.g. "Cluster-in.domain.tld" or "cluster-out.domain.tld", which is addressed by inbound and outbound emails. In the DNS, it is possible to specify multiple IP addresses to any host name. As a result, a simple Load balancing can be achieved.

If, for example, the internal email server requests for the email transmission given for specified hostname of SEPPmail cluster in the DNS, all this to host name assigned IP addresses are getting returned, but each time in a different order. The internal email server can now select one of these IP addresses to send the email to. In case of failure, the next lower priority cluster member system available in the cluster will respond. Figure 3 shows a logical representation of the scenario.

What happens in detail:

Each SEPPmail system has its own completely separate IP address, that can be accessed by only this system, for example, to configure settings that are not synchronized in the cluster.

In figure 3, these are the IP addresses 10.10.0.9 and 10.10.0.10.

In addition, there are two virtual IP addresses to combine the two SEPPmail systems logically into one group. In figure 3, these virtual IP addresses (groups) are shown separated by color.

The internal and the external email servers respond for the transmission of incoming and outgoing emails to the SEPPmail cluster system host name instead of a virtual IP address. If a request comes for this host name, set to the DNS server, then the host name is resolved in all set up IP addresses.

In our case, the resolved IP addresses correspond to the virtual cluster IP addresses as shown in Figure 3. The two virtual IP addresses have each a different system as a primary cluster member and secondary cluster member. This way, a redundancy is given in case of failure, since both cluster member systems monitor each other and one system can always take over the task of the failed system.

The virtual IP address 10.10.0.1, shown here in green, and the virtual IP address 10.10.0.2, here shown in orange, will be assigned the host names, e.g. registered in the internal email server for sending of outgoing emails. This host name is resolved to the following IP addresses:

```
cluster-out.domain.tld.   1800  IN  A  10.10.0.1
cluster-out.domain.tld.   1800  IN  A  10.10.0.2
```

At each resolution of the addressed host name »cluster-out.domain.tld«, the DNS server will return all assigned IP addresses, but in a different order.

```
cluster-out.domain.tld.   1800  IN  A  10.10.0.2
cluster-out.domain.tld.   1800  IN  A  10.10.0.1
```

The internal email server can now select an IP address and send the outgoing email. As with any request to change the order of the returned IP addresses, emails can be distributed to the available cluster member systems.

Summary:

© 2014 SEPPmail AG

With transmission of incoming and outgoing emails via the SEPPmail cluster, instead of a virtual cluster IP address, a host name will be assigned in the relevant email servers. This is then resolved at run-time in their corresponding IP addresses. Thus, the internal and external email server can send incoming and outgoing emails optionally to one of these resolved IP addresses. Since this is always about one virtual cluster IP addresses, the cluster member systems respond according to priority, e. g. in case of error.

The load balancing of incoming and outgoing email data flows can be achieved through the DNS Round-Robin function.

Source: Wikipedia, http://en.wikipedia.org/wiki/Round-robin_DNS (reproduced excerpts also in this chapter)

The set up of virtual IP addresses and assigning priorities is performed in accordance with steps in the »System« menu.

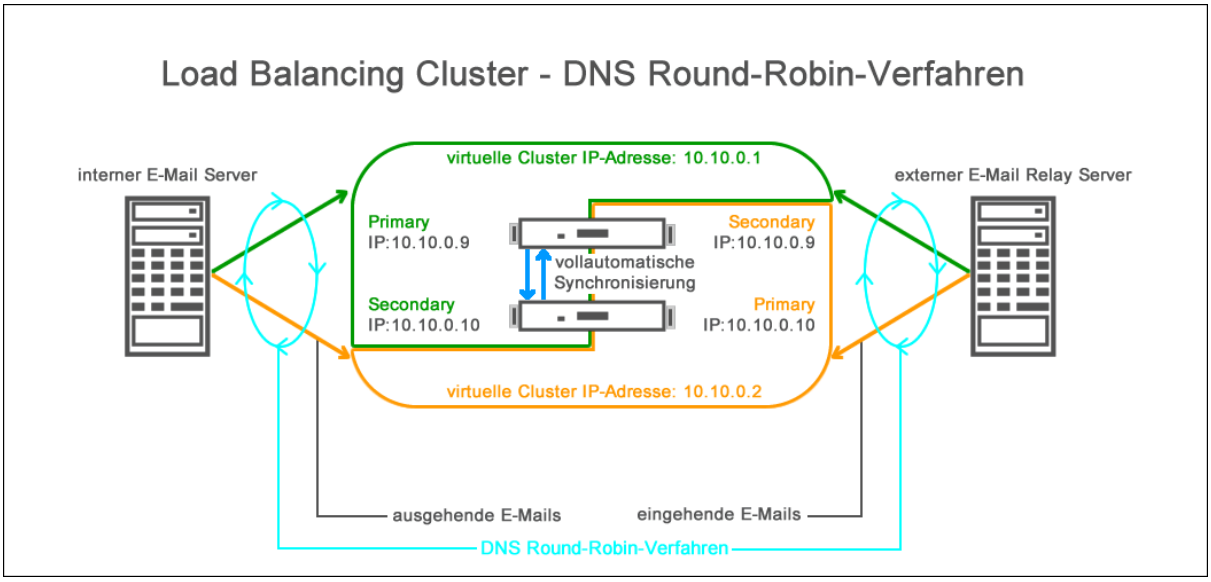


Figure 3 - Schematic representation of the load balancing through the DNS Round-Robin method for incoming and outgoing emails

Use with redundant internal and external MTAs (Mail Transport Agent)

In the SEPPmail configuration, can exactly one host to be configured as an external MTA (email relay). Analogously, for each internal email domain (email server), can exactly one internal MTA be configured. The SEPPmail system can support redundant external and internal MTAs with the methods explained in the following sections.

In the SEPPmail system, the external i.e. the internal MTA can be configured in several ways:

- Specifying an IP address
- Specifying a host name
- Specifying a domain, which is carried out for MX Lookup

The distinction between the IP address, host name and domain takes place by means of square brackets (»[« , »]«): IP addresses and host names must be enclosed in square brackets, domains for which an MX lookup is performed, without square brackets.

© 2014 SEPPmail AG

The SEPPmail system can support redundant external or internal MTAs by only internally available dummy domain, configured for the external and the internal MTA. For each dummy domain, MX records are created with 2 different preferences in the internal DNS. The SEPPmail system forwards emails as default on to the host with the lowest preference. In case of failure of that host, emails are automatically sent to the host with the higher preference.

The setting of the host name for the redundant internal and external MTAs, is performed in the »Mail System« menu.

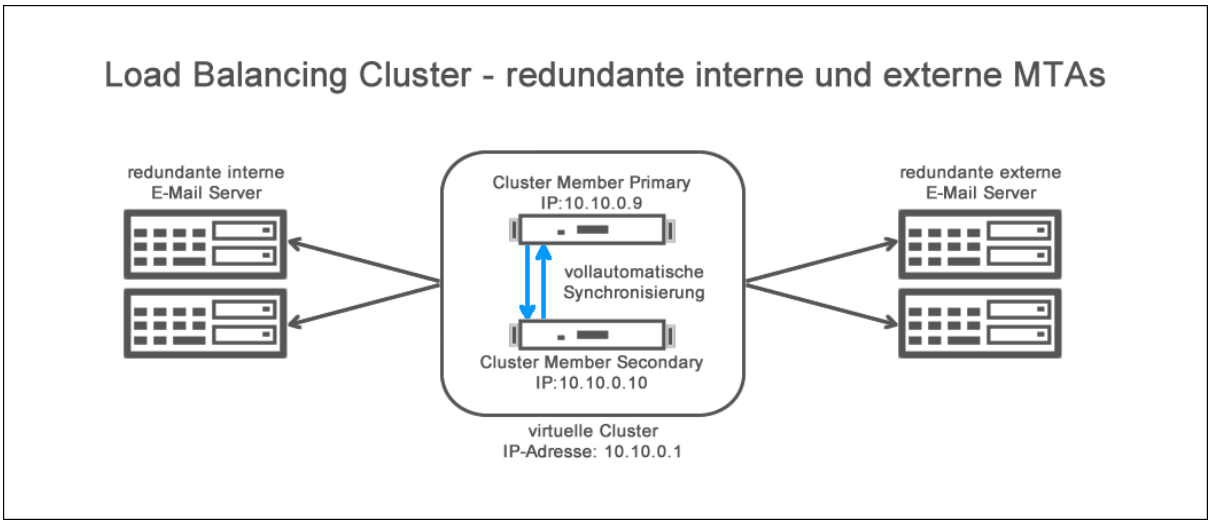


Figure 4 - Schematic representation of the use of internal and external redundant MTAs

© 2014 SEPPmail AG

6.10.4 Geo Cluster

A Geo-cluster (also called »Multisite System«) is used to replicate configuration databases between geographically distant SEPPmail systems in various locations of the company.

Example of use:

A company operates worldwide and for this reason, operates several data centers on different continents. The company sites are all connected through a VPN and have in each data center to access the Internet. Within this internal corporate network, there is a mail transport system, e.g. based on Microsoft Exchange or Lotus Notes. The externally sent emails can be sent to different Internet connections to the Internet, depending on the company internally mapped directive. (e.g. if an Internet access at one location does not work, the VPN connection between sites is not affected and thus the external transmission of emails is now performed via a different site)

This requires, that the necessary cryptographic email processing at all Internet access points is done the same. It must allow all user accounts and their certificates to be present to sign, decrypt, and encrypt and also the configuration settings must be identical with no deviations in the email processing methods.

Thanks to the Geo-Cluster function of the SEPPmail system, the configuration changes between all SEPPmail Geo-Cluster systems can be replicated immediately. Thus, a consistent configuration is ensured in all systems.

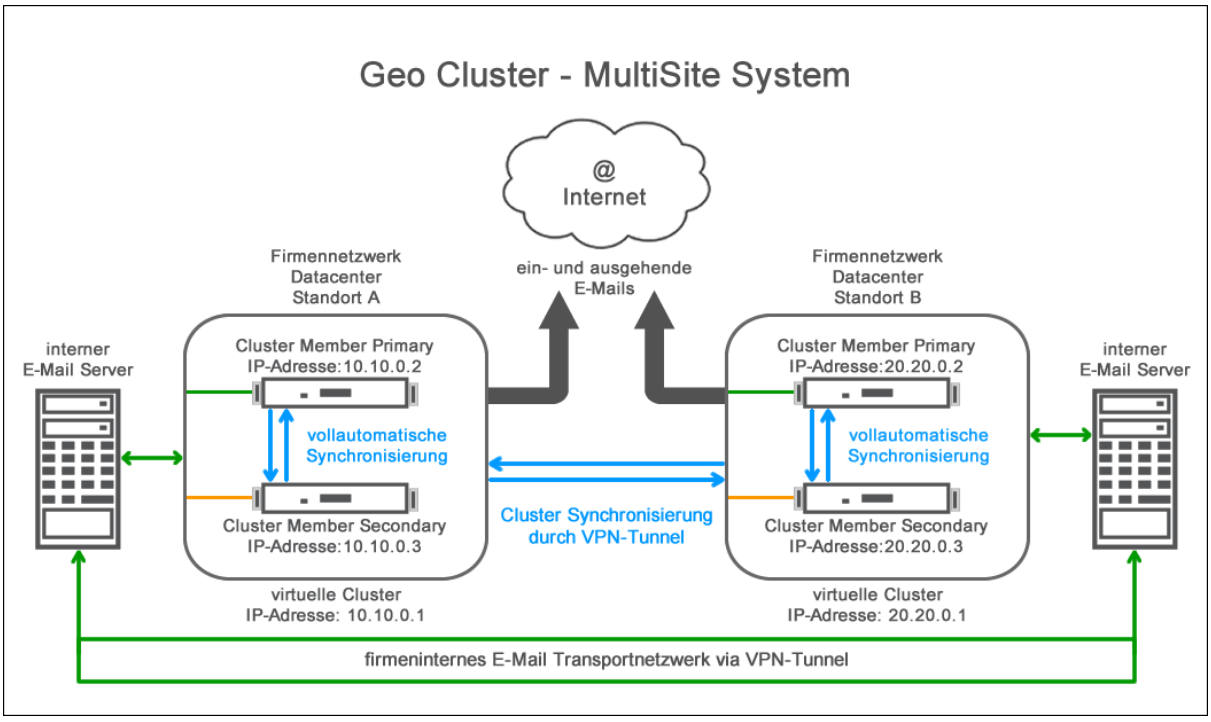


Figure 1 - Schematic representation of a Geo-Cluster structure

© 2014 SEPPmail AG

6.10.5 Frontend-Backend Cluster

Frontend-Backend cluster, where the front end systems have no local configuration database

Operating a SEPPmail system as a front end server is a very special cluster function. The difference with the normal function of the SEPPmail cluster system is, that even on the front end server itself, no configuration database exist.

The configuration data needed at runtime will be used as required, e.g. when necessary decrypting an incoming email, transferred from the cluster to the front end server and kept only temporarily. After the email processing, this configuration data is immediately deleted.

This function can be found in the corresponding usage scenario requirements on compliance.

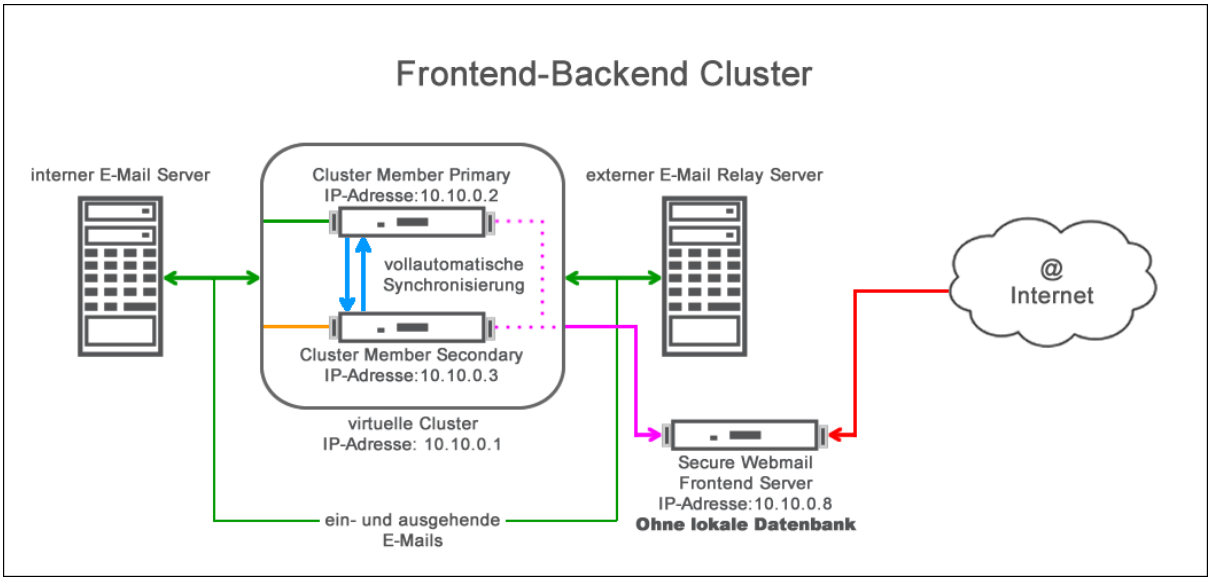


Figure 1 - Schematic representation of a Frontend-Backend cluster structure

© 2014 SEPPmail AG

6.10.6 Setting up a Cluster Configuration

Important note:

Please note the safety instructions, when you make changes to the parameters of the composite clusters, dissolve out systems of the cluster compound, replacing systems in case of failures or when adding new systems to the cluster compound.

Without considering these safety instructions, you may render the complete cluster compound unusable.

The safety instructions can be found in the chapter Safety Instructions 131.

Section	Parameter	Description
Prepare for Cluster	use this key to add a different device to this device/cluster	»Download Cluster Identifier« Button Select the »Download Cluster Identifier« button to download the native system RSA PRIVATE KEY and save the file locally. The downloaded file has the file name »clusterid.txt« . A cluster identification is needed to add another SEPPmail appliance to this unit and thus to form a cluster network.
Add this device to existing cluster WARNING: All data, except network configuration of this device will be lost	Cluster Identifier	Import in this box the »Cluster Identifier« file of an existing SEPPmail cluster system. The local system is added to the existing cluster. Please be aware about the safety instructions, when you add a new system to an existing cluster compound. Proceed to the further cluster setup only in case you completely understand the principle of setting up a clusters grouping! Without paying attention to the safety instructions, you can render the complete cluster compound unusable. The safety instructions can be found in the chapter Safety Instructions 131.
	Cluster Member IP	IP of the device you want to connect to. Do NOT use an IP alias address! Enter here the unique IP address of a SEPPmail system, which is already part of the cluster you want to add to this system. Do not use a virtual IP address of the cluster!

© 2014 SEPPmail AG

Section	Parameter	Description
		See »System > IP-Adresses« in the configuration interface. The connection of cluster systems is carried out via a secure shell connection to port TCP/22. Do not change this port setting.
	IP address of this device	IP address of other devices in the cluster can be used to connect to this device. Do NOT use an IP alias address! Enter here the unique IP address of the local system, which is to be added to the existing cluster. See »System > IP-Adresses« menu in the configuration interface. The connection of cluster systems is carried out via a secure shell connection to port TCP/22. Do not change this port setting.
	Connect	»Start« button Select the »Start«, button after you have entered all the necessary values for the corresponding parameters to start the cluster function on the local system. This system is now part of the cluster network.
Add this device as frontend server (no local database)	Cluster Identifier	Import in this box the »Cluster Identifier« file of an existing SEPPmail cluster systems. The local system is added to the existing cluster as a special frontend server.
	Existing Appliance IP	IP (or virtual IP) of the device (or cluster) you want to connect to. Enter here the unique IP address or the virtual cluster IP address of a SEPPmail system, which is already part of the cluster, that you also want to add this system. The connection of cluster systems is carried out via a secure shell connection to port TCP/22. Do not change this port setting.
	Connect	»Start« button Select the »Start« button, after you have entered all the necessary values for the corresponding parameters to start the clustering on the local

© 2014 SEPPmail AG

Section	Parameter	Description
		system. This system is now part of the cluster grouping as a frontend server.

Reference of the parameter menu under the »Cluster« menu item

6.10.6.1 Overview

The procedure for setting up and operation of a SEPPmail cluster is described in this chapter. The configured SEPPmail cluster consists of two systems in our configuration example. All necessary configuration steps are described in detail in the following sections of this chapter.

Configuration steps:

1. Set up the first SEPPmail system completely

2. Set up the second SEPPmail system

3. In the second SEPPmail system, only the settings in the »System« menu, the registration of the system menu »Administration« and import the SSL device certificate in the »SSL« menu are required, all other settings, such as the settings in the »Mail Processing« menu and more will be automatically entered, when creating the cluster.

4. In a virtualised environment, a second virtual appliance must be imported. This must not be a duplicate of the existing first instance.

5. Download the cluster identification in the first SEPPmail system.

6. Add the second SEPPmail system to the cluster.

7. Definition and configuration of the virtual IP address (es) of the cluster. Depending on the operating mode of the cluster, one or two virtual IP addresses are required.
   If the cluster is operated as a pure high availability cluster (failover cluster) (no division of the incoming and outgoing email data flow), then only one virtual cluster IP address is required.

   If the cluster is additionally configured for load balancing to increase the performance, then two virtual cluster IP addresses are required.
   Also in this operation mode, high availability cluster with additional load balancing, failover behavior of the cluster remains.

6.10.6.2 Safety notes

When you add a newSEPPmail system to an existing cluster composite or create a composite cluster for the first time, the entire existing cluster configuration will be replicated to this new cluster member system and then become constantly synchronized with the cluster compound.

All data on this system is lost, with the exception of the settings in the »System« and »SSL« menus, as well as the log files and statistics in the »Logs«, »Webmail Logs« and »Statistics« menus.

This is important, if data, such as S/MIME certificates, PGP keys, GINA user accounts e.g. are still needed on this system.

© 2014 SEPPmail AG

Furthermore, it is very important to understand the order in which SEPPmail systems need to be added to an existing cluster composite, i.e. which system is the replication source and which system is the replication target. If you confuse these systems, when creating a new cluster interconnection, it can happen that an existing and set up SEPPmail system is overwritten with blank data of the newly added system. This is even more important in case of an existing cluster group already consisting of several cluster member systems. This confusion between the replication source and replication target in this case may cause overriding the entire cluster compound with empty data of the new system.

The entire cluster compound would then become useless. Please consider this in the configuration.

© 2014 SEPPmail AG

6.10.6.3 Configuration of the VMware ESX environment

For the establishment and operation of a SEPPmail cluster based virtual machines in a VMware ESX environment, it is necessary to set up the security settings on the vSwitch and the corresponding port groups as follows:

In the the VMware vSphere Client, select »Inventory -> ESX-Server -> [Configuration tab] -> Network«

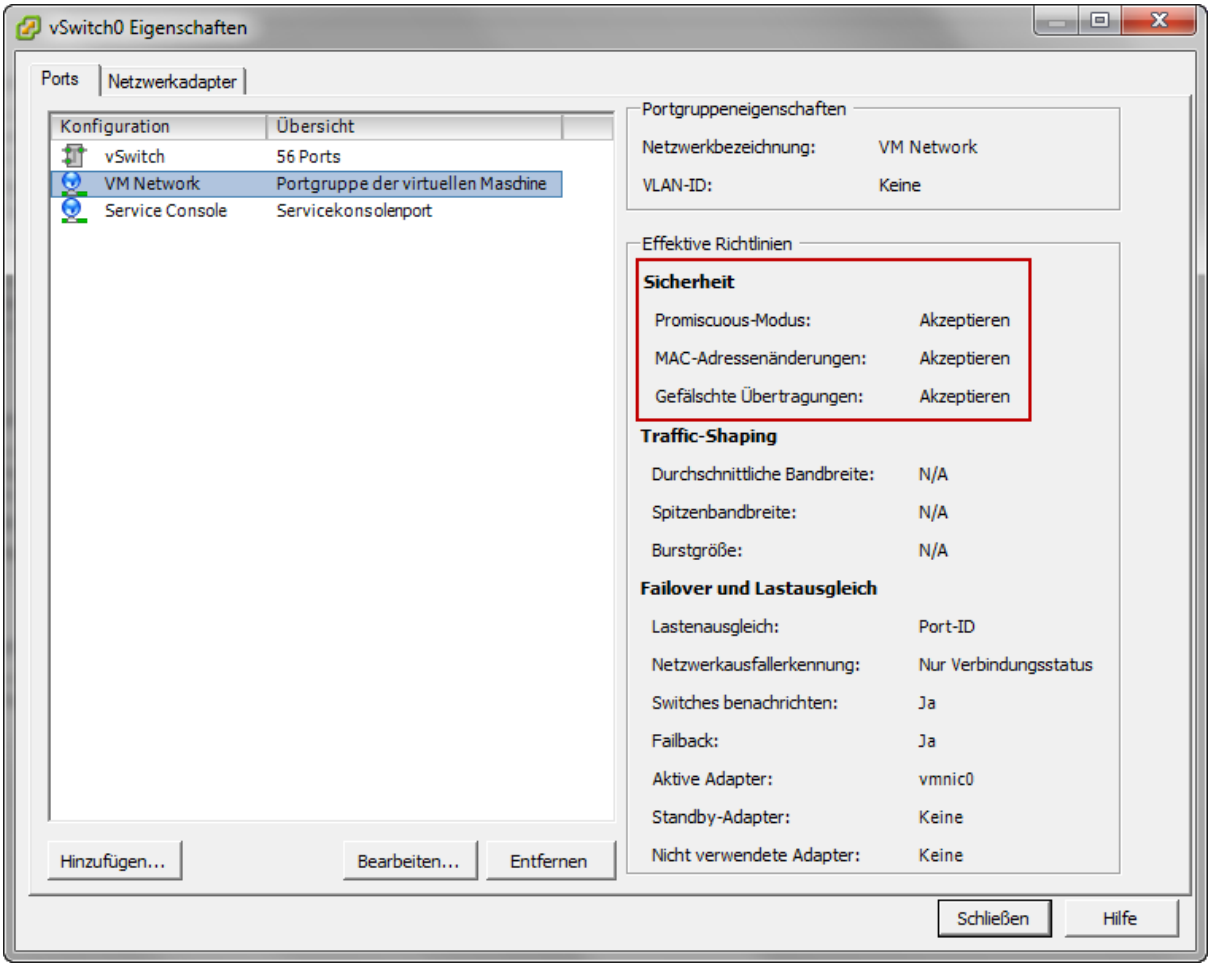


Figure 1 - Security setting for the port groups a in vSwitch of VMware ESXsystem

© 2014 SEPPmail AG

6.10.6.4 Setting up the basic settings of a SEPPmail system

To set up a SEPPmail cluster system, some basic settings must be carried out on the associated systems. All other settings are automatically replicated in the construction of a cluster or adding a new SEPPmail system to an existing cluster to the new cluster member. Thereafter all cluster member systems synchronize with each other, if a change of the configuration parameters, or transaction data occurs on a cluster member system. The transaction data includes PGP and S/MIME user certificates/ domain certificates and X.509 root certificates.

The basic settings include the following static system-specific configuration parameters, that are not replicated and synchronized among the cluster member systems:

- all settings in the »System« menu
- the SSL device certificate in the »SSL« menu
- the system license and the registration data of the system

The log files and statistics in the »Logs«, »Webmail Logs« and »Statistik« menus are also system-specific and are not replicated. All other configuration parameters are replicated between the cluster member systems and synchronized at each change.

6.10.6.5 Setting up the SEPPmail cluster systems

The first SEPPmail system of a cluster must be completely set up. See Chapter SEPPmail 13

The second SEPPmail system must be set up with the basic settings. This includes the network configuration and the registry of the system. See Chapter SEPPmail system 134

6.10.6.6 Downloading cluster identification

A cluster identification is needed to add another SEPPmail system to an existing cluster or compound to form a cluster composite of two SEPPmail systems.

To download a cluster identification, select in the configuration interface, the »Cluster« menu. Then select the »Download Cluster Identifier« button in the »Prepare for Cluster« section. You will get a »Save file« dialog and can save the cluster identification file locally as »clusterid.txt«.

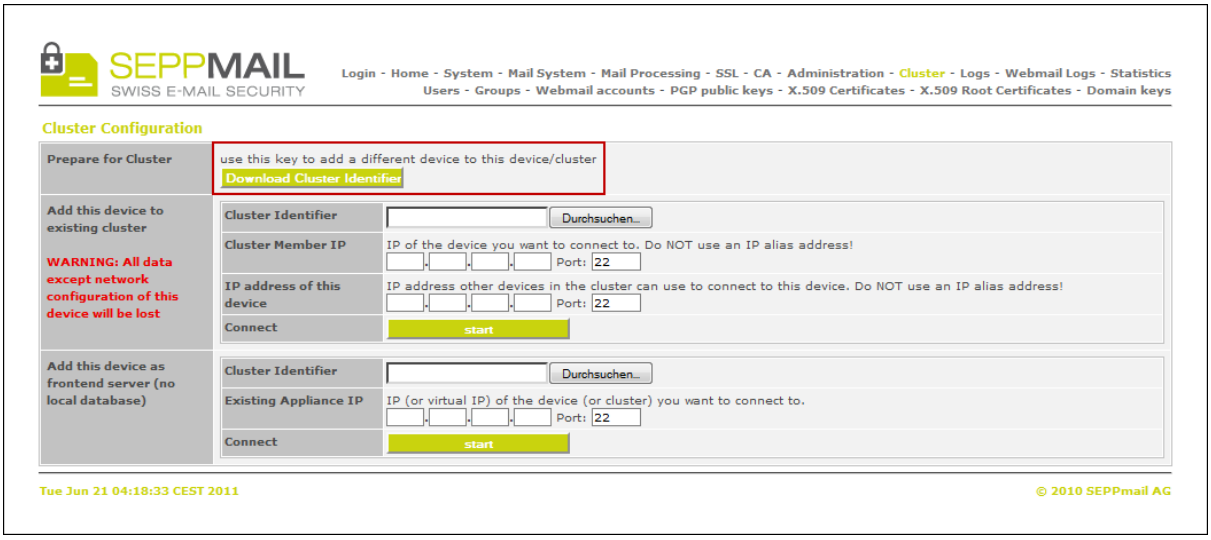

SEPPMAIL
SWISS E-MAIL SECURITY
Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys
Cluster Configuration
Prepare for Cluster
use this key to add a different device to this device/cluster
Download Cluster Identifier
Add this device to existing cluster
WARNING: All data except network configuration of this device will be lost
Cluster Identifier
Durchsuchen...
Cluster Member IP
IP of the device you want to connect to. Do NOT use an IP alias address!
Port: 22
IP address of this device
IP address other devices in the cluster can use to connect to this device. Do NOT use an IP alias address!
Port: 22
Connect
start
Add this device as frontend server (no local database)
Cluster Identifier
Durchsuchen...
Existing Appliance IP
IP (or virtual IP) of the device (or cluster) you want to connect to.
Port: 22
Connect
start
Tue Jun 21 04:18:33 CEST 2011
© 2010 SEPPmail AG

Figure 1 - Download the cluster identification

© 2014 SEPPmail AG

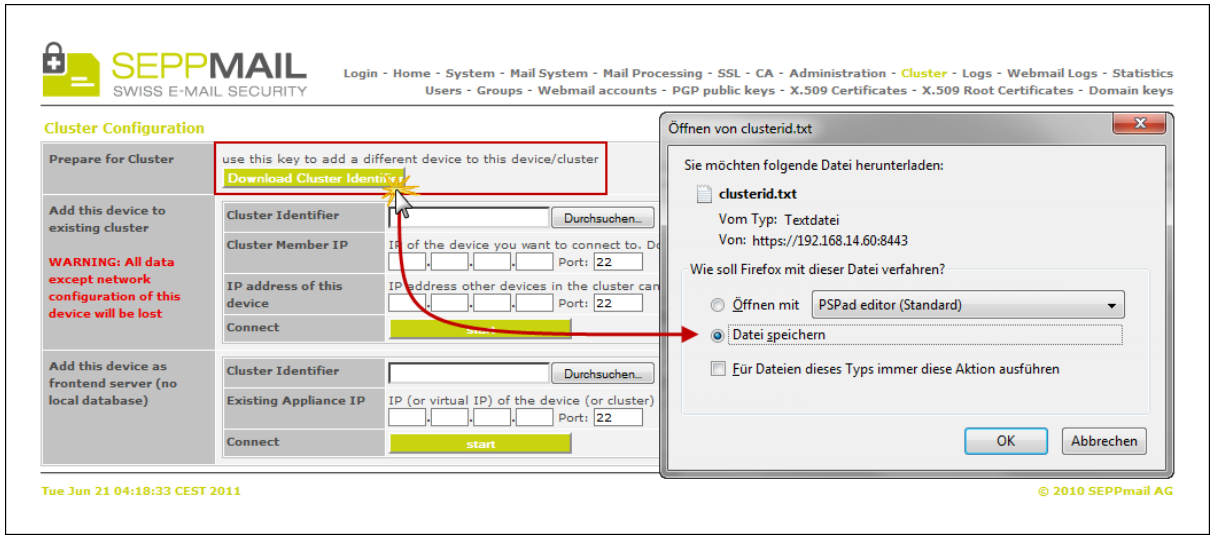

SEPPMAIL
SWISS E-MAIL SECURITY
Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys
Cluster Configuration
Prepare for Cluster
use this key to add a different device to this device/cluster
Download Cluster Identifier
Add this device to existing cluster
WARNING: All data except network configuration of this device will be lost
Cluster Identifier
Durchsuchen...
Cluster Member IP
Port: 22
IP address of this device
Connect
Add this device as frontend server (no local database)
Existing Appliance IP
IP (or virtual IP) of the device (or cluster)
start
Tue Jun 21 04:18:33 CEST 2011
© 2010 SEPPmail AG
Öffnen von clusterid.txt
Sie möchten folgende Datei herunterladen:
clusterid.txt
Vom Typ: Textdatei
Von: https://192.168.14.60:8443
Wie soll Firefox mit dieser Datei verfahren?
Öffnen mit
PSPad editor (Standard)
Datei speichern
Für Dateien dieses Typs immer diese Aktion ausführen
OK
Abbrechen

Figure 2 - Download Cluster Identification and save locally

© 2014 SEPPmail AG

6.10.6.7 Setting up SEPPmail cluster

To set up a SEPPmail cluster, you need at least two systems. In principle, there is no limit to the number cluster members systems. You can easily operate 10 systems or more in a cluster compound. This cluster compound can all be set up so, that each of them is implemented using specific requirements, so that all of the four modes may be used.

The primary means of a SEPPmail cluster consisting of at least two systems, is working the same way, as adding additional cluster member systems.

To add a SEPPmail appliance to an existing cluster (or to set up a cluster for the first time), select the »Cluster« menu item in the configuration interface.

To build the cluster, the fields in the »Add this device to existing cluster« section must be filled. Proceed as follows::

1. Select the »Cluster Identifier« parameter file with the cluster identification, that you have downloaded.
2. Enter for the »Cluster Member IP« parameter the (physical) IP address of the first SEPPmail appliance, the one to which you want to add this system. If there are already several appliances in the cluster, the (physical) IP address of a cluster member system is sufficient.
3. Enter for the »IP address of this device« parameter the own (physical) IP address, under which this appliance is accessible for other appliances in the cluster.
4. Check all previously entered values. Connect to the process by selecting the »start« button. The cluster compound is now created i.e. extended, so that the existing cluster configuration replicated to include the new cluster member system. All of the subsequent configuration changes in the cluster will now automatically and immediately be synchronized with the newly added cluster member system.

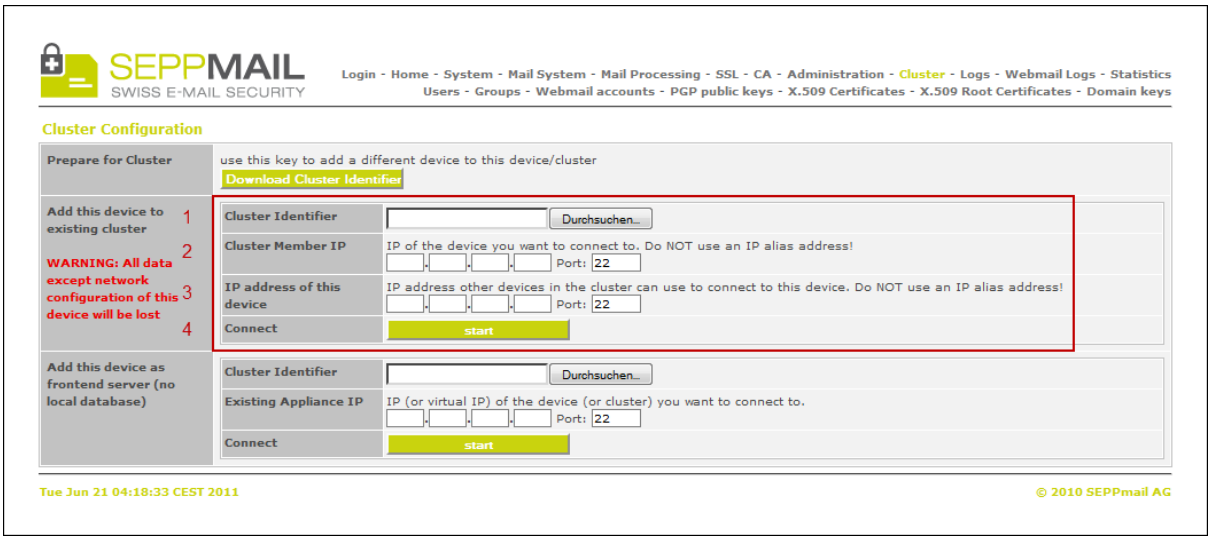

SEPPMAIL
SWISS E-MAIL SECURITY
Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys
Cluster Configuration
Prepare for Cluster
use this key to add a different device to this device/cluster
Download Cluster Identifier
Add this device to existing cluster
1
2
WARNING: All data except network configuration of this device will be lost
3
4
Cluster Identifier
Durchsuchen...
Cluster Member IP
IP of the device you want to connect to. Do NOT use an IP alias address!
Port: 22
IP address of this device
IP address other devices in the cluster can use to connect to this device. Do NOT use an IP alias address!
Port: 22
Connect
start
Add this device as frontend server (no local database)
Cluster Identifier
Durchsuchen...
Existing Appliance IP
IP (or virtual IP) of the device (or cluster) you want to connect to.
Port: 22
Connect
start
Tue Jun 21 04:18:33 CEST 2011
© 2010 SEPPmail AG

Figure 1 - Adding a SEPPmail appliance to an existing cluster or first-time creation of a cluster

After the cluster network was created, the display in the »Cluster« menu changes and it now reflects the status of the cluster compound. If you want to remove this system from the cluster compound

© 2014 SEPPmail AG

again, you choose the »remove this device from cluster« button in the »remove from cluster« section.

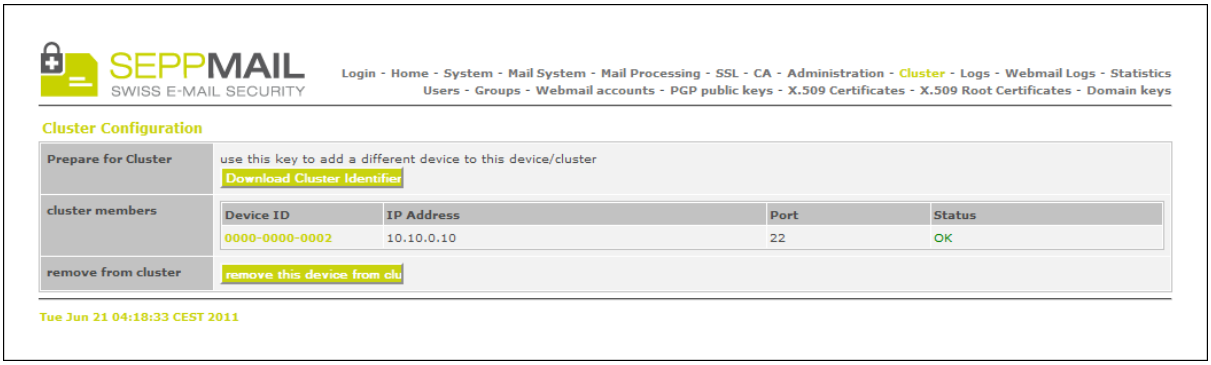

SEPPMAIL
SWISS E-MAIL SECURITY
Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys
Cluster Configuration
Prepare for Cluster
use this key to add a different device to this device/cluster
Download Cluster Identifier
cluster members
Device ID
IP Address
Port
Status
0000-0000-0002
10.10.0.10
22
OK
remove from cluster
remove this device from clu
Tue Jun 21 04:18:33 CEST 2011

Figure 2 - Cluster state of the first cluster member system

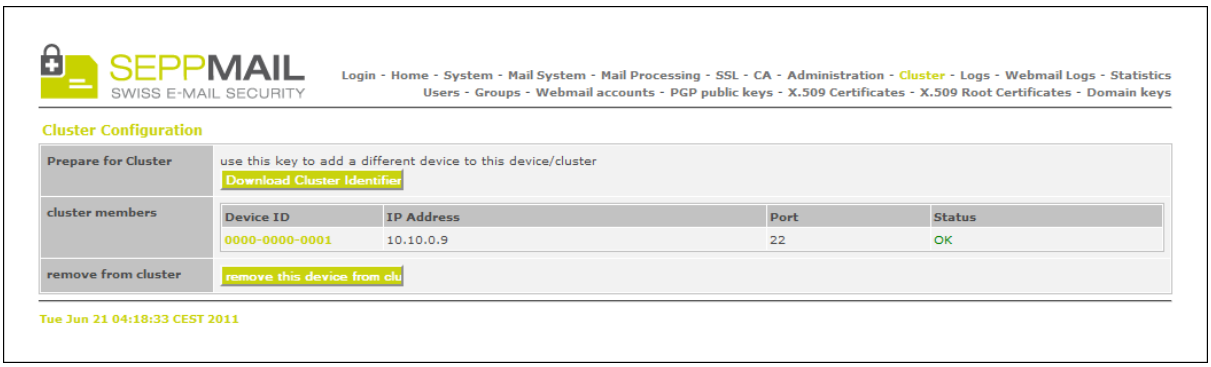

SEPPMAIL
SWISS E-MAIL SECURITY
Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys
Cluster Configuration
Prepare for Cluster
use this key to add a different device to this device/cluster
Download Cluster Identifier
cluster members
Device ID
IP Address
Port
Status
0000-0000-0001
10.10.0.9
22
OK
remove from cluster
remove this device from clu
Tue Jun 21 04:18:33 CEST 2011

Figure 3 - cluster state of the second cluster member system

When you add a SEPPmail system to an existing cluster or compound or, create a compound cluster for the first time, the entire existing cluster configuration is replicated to this new cluster member system and is thereafter constantly synchronized with the cluster compound.

All data on this system is lost, with the exception of the settings in the »System« and »SSL« menus, as well as the log files and statistics in the »Logs«, »Webmail Logs« and »Statistics« menus.

This is important because, this system's configuration data may still be needed, such as S/MIME certificates, PGP keys, Secure Webmail accounts etc..

Furthermore, it is very important to understand the order in which the SEPPmail systems need to be added to an existing cluster or compound, which system is the replication source and which system is the replication target. If you confuse these systems, when creating a new cluster interconnection, it may happen, that an existing and set up SEPPmail system is overwritten with the »empty data« of the newly added system. This is even more important in an existing cluster compound, if it is already composed of several cluster member systems. This confusion between the replication source and replication target in this case means, that the existing cluster association will be overwritten with the new system's »empty data«.

© 2014 SEPPmail AG

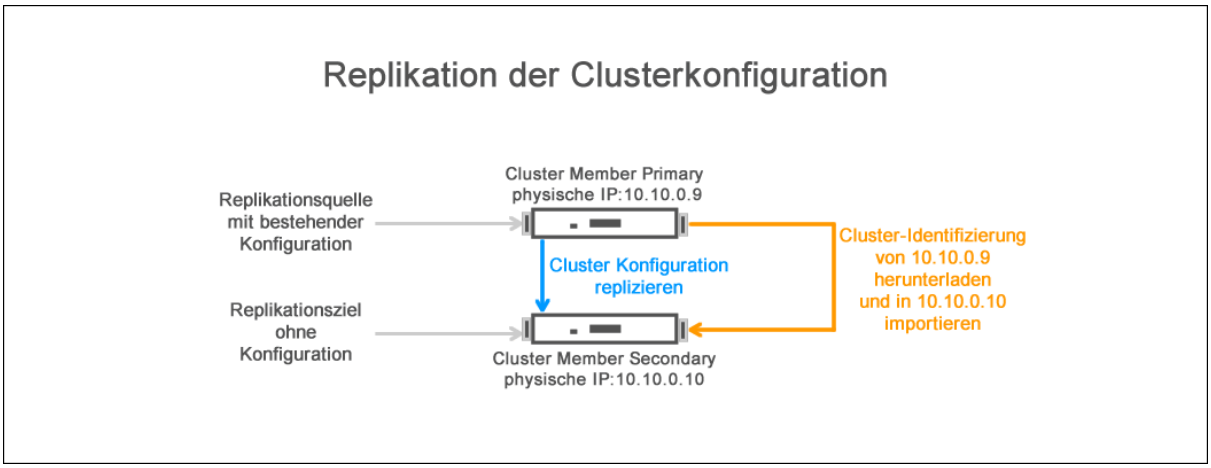


Figure 4 - Schematic representation of the replication of the cluster configuration between two SEPPmail cluster member systems

Until now, you have set up the primary replication and then following synchronization of the configuration data, between the cluster member systems. To set up a high-availability cluster and a load balancing cluster, it is necessary to aggregate the individual cluster member systems under one or more virtual cluster IP addresses.

© 2014 SEPPmail AG

6.10.6.8 Setting up High Availability Cluster

When setting up a high-availability cluster, two different functions are needed.

In the »Cluster« menu in the configuration interface, the replication, and then following the synchronization of the configuration information of the cluster configuration between cluster member systems, are to be set up and to be activated. We have already discussed this point in the previous chapter.

In the »System« menu, in the configuration interface, the monitoring of the cluster member systems with each other, and the priorities of the individual cluster member systems are to be set up within the cluster.

The configuration of the virtual cluster IP address(es) follows in the »System« (Advanced View) menu item in the »IP ALIAS Addresses« section. This configuration must be made in each cluster member system, which is part of the cluster.

When configured for operation, as a pure high availability cluster (failover cluster), the same virtual cluster IP address is configured in the cluster member systems. A system must thereby be configured with the »Primary« priority and another system must be configured with the »Backup« priority. See figure 1 and figure 2. We use the IP addresses from the presentation in the chapter High Availability Cluster 118.

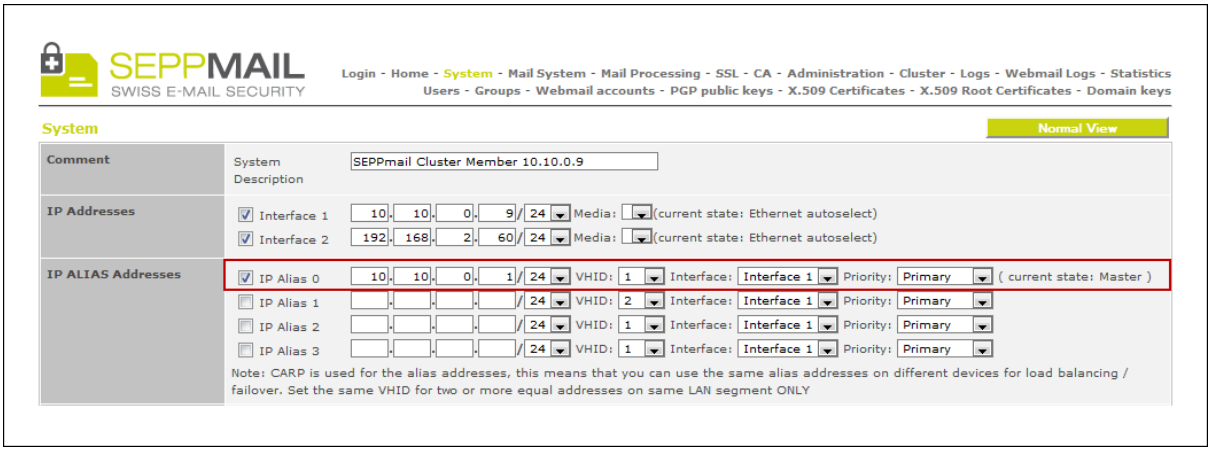
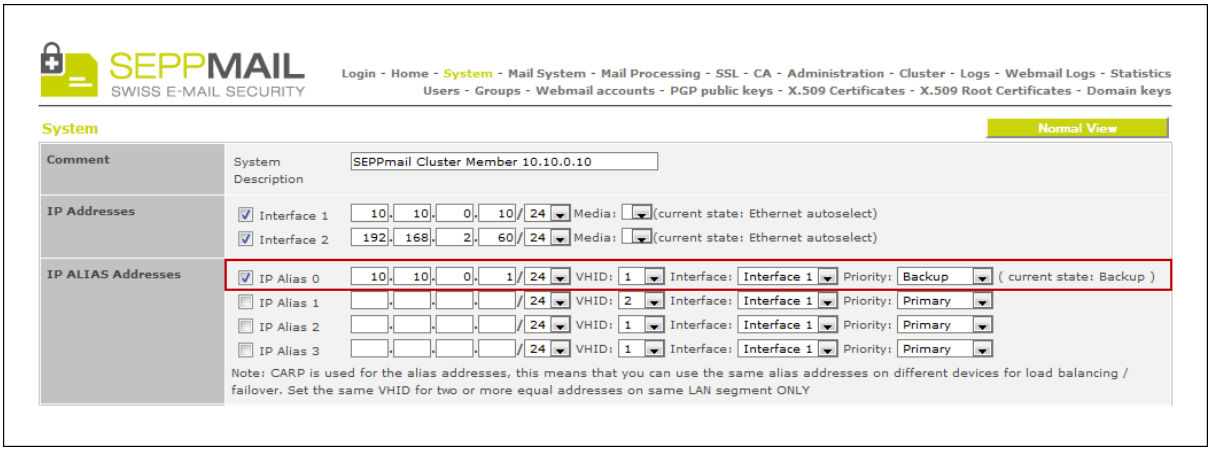

SEPPMAIL
SWISS E-MAIL SECURITY
Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys
System
Normal View
Comment
System Description
SEPPmail Cluster Member 10.10.0.9
IP Addresses
Interface 1 10.10.0.9/24 Media: (current state: Ethernet autoselect)
Interface 2 192.168.2.60/24 Media: (current state: Ethernet autoselect)
IP ALIAS Addresses
IP Alias 0 10.10.0.1/24 VHID: 1 Interface: Interface 1 Priority: Primary (current state: Master)
IP Alias 1 /24 VHID: 2 Interface: Interface 1 Priority: Primary
IP Alias 2 /24 VHID: 1 Interface: Interface 1 Priority: Primary
IP Alias 3 /24 VHID: 1 Interface: Interface 1 Priority: Primary
Note: CARP is used for the alias addresses, this means that you can use the same alias addresses on different devices for load balancing / failover. Set the same VHID for two or more equal addresses on same LAN segment ONLY

Figure 1 - High availability cluster - Virtual cluster IP address of the first SEPPmail cluster member system


SEPPMAIL
SWISS E-MAIL SECURITY
Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys
System
Normal View
Comment
System Description
SEPPmail Cluster Member 10.10.0.10
IP Addresses
Interface 1 10.10.0.10/24 Media: (current state: Ethernet autoselect)
Interface 2 192.168.2.60/24 Media: (current state: Ethernet autoselect)
IP ALIAS Addresses
IP Alias 0 10.10.0.1/24 VHID: 1 Interface: Interface 1 Priority: Backup (current state: Backup)
IP Alias 1 /24 VHID: 2 Interface: Interface 1 Priority: Primary
IP Alias 2 /24 VHID: 1 Interface: Interface 1 Priority: Primary
IP Alias 3 /24 VHID: 1 Interface: Interface 1 Priority: Primary
Note: CARP is used for the alias addresses, this means that you can use the same alias addresses on different devices for load balancing / failover. Set the same VHID for two or more equal addresses on same LAN segment ONLY

© 2014 SEPPmail AG

Figure 2 - High availability cluster - Virtual cluster IP address of the second SEPPmail cluster member system

The two cluster member systems are now combined under one virtual cluster IP address. If this cluster IP address is addressed, the system will respond with the »Primary« priority. If this system is not available, the system responds with the «Backup« priority. An automatic change of status is performed, when the primary system is not available. The system with the »Backup« status gets its previous state automatically, when the primary system becomes available again. In this case, it is guaranteed, that in the event of a fault, incoming and outgoing emails continue to be processed, and no interference will occur in the email data flow.

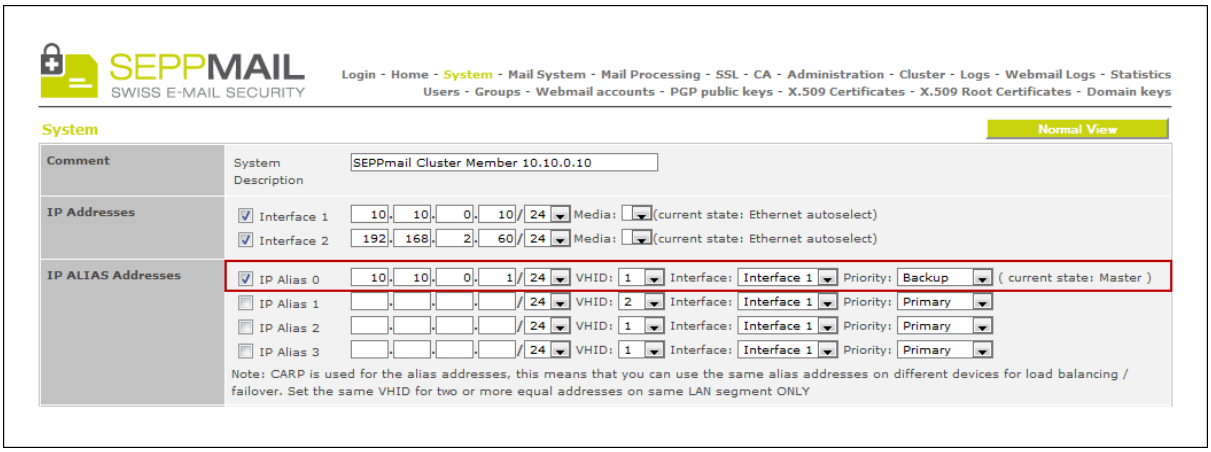

SEPPMAIL
SWISS E-MAIL SECURITY
Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys
System
Normal View
Comment
System Description
SEPPmail Cluster Member 10.10.0.10
IP Addresses
Interface 1
10 . 10 . 0 . 10 / 24
Media:
(current state: Ethernet autoselect)
Interface 2
192 . 168 . 2 . 60 / 24
Media:
(current state: Ethernet autoselect)
IP ALIAS Addresses
IP Alias 0
10 . 10 . 0 . 1 / 24
VHID: 1
Interface: Interface 1
Priority: Backup
(current state: Master)
IP Alias 1
/ 24
VHID: 2
Interface: Interface 1
Priority: Primary
IP Alias 2
/ 24
VHID: 1
Interface: Interface 1
Priority: Primary
IP Alias 3
/ 24
VHID: 1
Interface: Interface 1
Priority: Primary
Note: CARP is used for the alias addresses, this means that you can use the same alias addresses on different devices for load balancing / failover. Set the same VHID for two or more equal addresses on same LAN segment ONLY

Figure 4 - High availability cluster - automatic change of status of the secondary system (the primary cluster member system is not available)

Thus, the cluster configuration is complete. When using a cluster, note the following:

- When routing emails to the SEPPmail cluster, the virtual cluster IP address should always be addressed.
- In internal email server and in the external MTA, all IP addresses of the cluster must be authorized to deliver emails, i.e. all physical and virtual IP addresses of the SEPPmail cluster (Email Relay settings of the respective components).
- In the firewall, all the IP addresses of the cluster must be entitled to an SSH connection (port TCP/22) to build the update server in the SEPPmail data center, i.e. all physical and virtual IP addresses of the SEPPmail cluster.
- In a cluster, the configurations of the two SEPPmail systems are automatically synchronized (with the exception of the settings in the »System« menu)

© 2014 SEPPmail AG

6.10.6.9 Setting up Load Balancing cluster

The additional set up of a load balancing cluster requires an already functional set up high availability cluster. A load-balancing cluster divides the data flow for inbound and outbound emails each to appropriate cluster members system and enables an optimal utilization of the existing system resources.

Each group of cluster member systems receive, in addition to the single physical IP addresses of the individual systems, a virtual IP address. In dependence on the priority assigned, the systems will react with response to the virtual cluster IP address. If two or more cluster member systems have the same priority in the cluster network, the systems will respond in the order, in which they were started.

In this documentation, a cluster composite is shown for two SEPPmail systems. You can also set up a cluster of three or more systems. In this case, each virtual cluster IP address is to be applied as an additional alias IP address.

When configured for operation as a high availability cluster (failover cluster) with distribution of incoming and outgoing email data flow (load balancing cluster) in the cluster member systems are configured with at least two virtual cluster IP addresses.

A virtual cluster IP address for the incoming email data flow (IP alias 0) and another virtual cluster IP address (IP Alias 1) for the outgoing email data flow. Thus, the failure of a cluster member system ensures, that the second system can take over the function of the failed system. A cluster member system must then be configured with the »Primary« priority and a cluster member system with the »Backup« priority. The priorities must be assigned for each virtual IP address oppositely.

Each cluster member system is now associated with two (or more, if, for example, three systems are used) IP alias addresses as a virtual cluster IP address. The individual cluster member systems react differently depending on the set priority to each virtual cluster IP address. If a system fails, the remaining system can always work as a backup system.

In addition, a unique »Virtual Host ID« must be assigned for each virtual cluster IP address, because we have bound more than one alias IP address for each cluster member system. (the »VHID« must be identical to the corresponding virtual cluster IP address on each system)

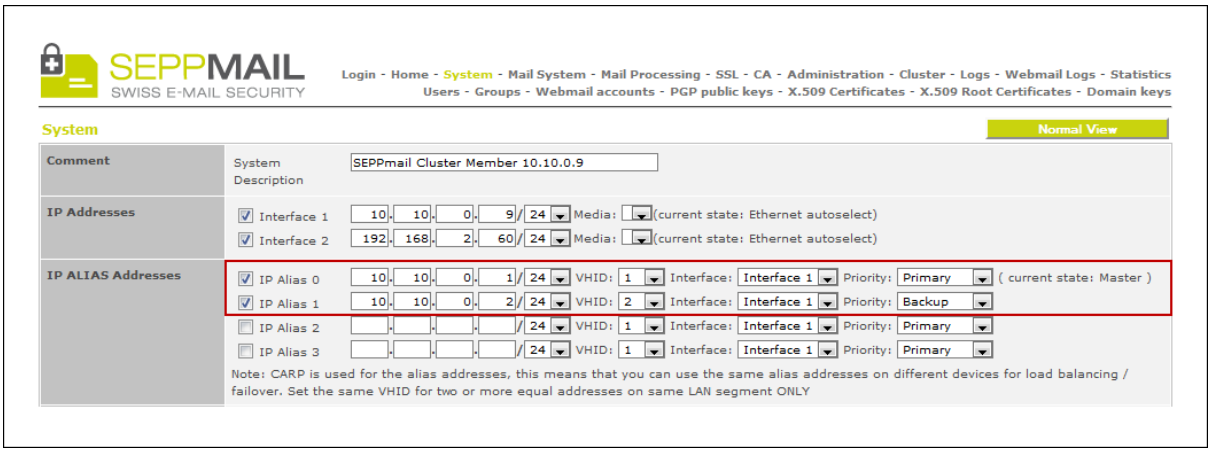

SEPPMAIL
SWISS E-MAIL SECURITY
Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys
System
Normal View
Comment
System Description
SEPPmail Cluster Member 10.10.0.9
IP Addresses
Interface 1 10 10 0 9 / 24 Media: (current state: Ethernet autoselect)
Interface 2 192 168 2 60 / 24 Media: (current state: Ethernet autoselect)
IP ALIAS Addresses
IP Alias 0 10 10 0 1 / 24 VHID: 1 Interface: Interface 1 Priority: Primary (current state: Master)
IP Alias 1 10 10 0 2 / 24 VHID: 2 Interface: Interface 1 Priority: Backup
IP Alias 2 / 24 VHID: 1 Interface: Interface 1 Priority: Primary
IP Alias 3 / 24 VHID: 1 Interface: Interface 1 Priority: Primary
Note: CARP is used for the alias addresses, this means that you can use the same alias addresses on different devices for load balancing / failover. Set the same VHID for two or more equal addresses on same LAN segment ONLY

Figure 5 - High Availability cluster with additional load distribution - two virtual cluster IP addresses of the first SEPPmail cluster member system

© 2014 SEPPmail AG

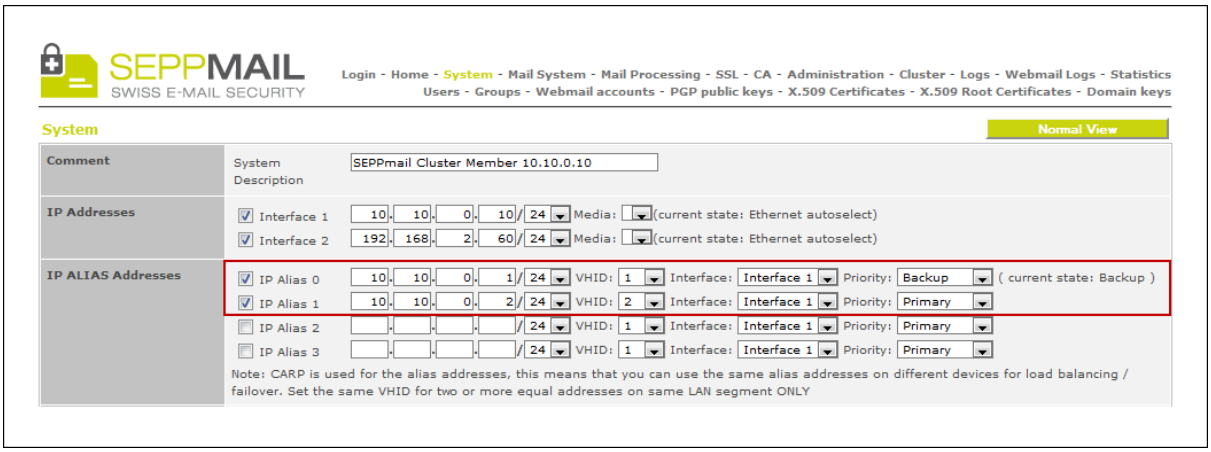

SEPPMAIL
SWISS E-MAIL SECURITY
Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys
System
Normal View
Comment
System Description
SEPPmail Cluster Member 10.10.0.10
IP Addresses
Interface 1
Interface 2
Media:
(current state: Ethernet autoselect)
IP ALIAS Addresses
IP Alias 0
IP Alias 1
IP Alias 2
IP Alias 3
VHID:
Interface:
Priority:
Backup
Primary
(current state: Backup)
Note: CARP is used for the alias addresses, this means that you can use the same alias addresses on different devices for load balancing / failover. Set the same VHID for two or more equal addresses on same LAN segment ONLY

Figure 6 - High Availability cluster with additional load distribution - two virtual cluster IP addresses of the 2nd SEPPmail cluster member system

Thus, the cluster configuration is complete. When using a cluster, note the following:

- When routing emails for SEPPmail cluster, the virtual cluster IP address should always be addressed.
- In internal email server and in the external MTA, all IP addresses of the cluster must be authorized to deliver emails, i.e. all physical and virtual IP addresses of the SEPPmail cluster (Email Relay settings of the respective components).
- In the firewall, all the IP addresses of the cluster, must be entitled to an SSH connection (port TCP/22) to build the update server in the SEPPmail data center, i.e. all physical and virtual IP addresses of the SEPPmail cluster.
- In a cluster, the configurations of the two SEPPmail systems are automatically synchronized (with the exception of the settings in the »System« menu)

© 2014 SEPPmail AG

6.10.6.10 Setting up Geo Cluster

Using a Geo Cluster, a local SEPPmail cluster can automatically synchronize itself with ones located in several different geographic locations of a company with their configuration data.

Consider the application of a geographic cluster in the following scenario:

A company may, in addition to the company headquarters, have several geographically separate locations and be connected between these sites via VPN. The internal communication within the company is mapped on an enterprise-wide group ware system.

Each geographic location has, for example, an Internet connection for the local sending and receiving emails. Each site operates its own groupware servers, that are connected with each other. The company's internal email communication is mapped on this own email transport network.

Each geographic location can send and receive their emails through an Internet connection. A dynamic email routing, that in principle enables emails to be sent or received at all locations through the company's internal email transport network. This requires at each location a private SEPPmail cluster for email signature and to encrypt and decrypt emails.

The SEPPmail clusters, set up at each site locally, are set up in each case as high availability clusters. Each cluster in the different locations would thus be an independent, but locally limited system, in which the cluster member systems are monitoring each other and synchronizing their configurations with each other.

To further establish global synchronization of the individual clusters of systems between geographically separate locations, we can set up a Geo Cluster, or a »MultiSite System«. A Geo Cluster synchronizes configurations between the local cluster systems of separate geographical locations to a global SEPPmail cluster system. Such a system is referred to as Geo Cluster. It links all the local cluster systems of geographically separate locations to a company-wide Geo cluster.

In this Geo Cluster, all configuration changes will become attached to a SEPPmail cluster member system and are performed automatically to be synchronized to all cluster member systems in all locations. This ensures that, at all times, the required data, such as new user accounts, including user certificates, or secure web mail accounts on all cluster member systems are available. Manual configuration of each system or manual synchronization of the configuration between the cluster member systems is no longer necessary and reduces the administrative configuration effort.

How is a Geo Cluster set up?

When setting up a Geo Cluster, a cluster member system at Site B is added to a cluster member system of location A. These cluster member systems are not connected via a virtual cluster IP address, such as High Availability and Load Balancing Cluster. There is only the synchronization of the configuration data.

To do this, proceed as described in the chapters Downloading Cluster Identification 134 and SEPPmail cluster 136.

6.10.6.11 Setting up Frontend-Backend cluster

If you want to run a newly added SEPPmail system for safety reasons without a local database (e.g. user certificates, domain certificates, etc.), you can add the new system as an alternative front end server. The actual configuration and user data is located on the other SEPPmail systems, that operate as a back end server appliances. To do this, select the »Cluster« menu item in the configuration interface.

© 2014 SEPPmail AG

To add the new SEPPmail system as front end server to an existing cluster, the fields in the »Add this device as frontend server (no local database)« section must be filled. Proceed as follows:

1. Select for the »Cluster Identifier« parameter the file with the cluster identification, which have you downloaded. See the chapter Download cluster identification 134.
2. Enter for the »Existing Appliance IP« parameter the physical IP address of the cluster member system i.e. the alias IP address of the existing cluster grouping on to which you want to connect.
3. Check all previously entered values. Connect through the process selecting from the »start« button.

No adjustment is necessary on the back end servers.

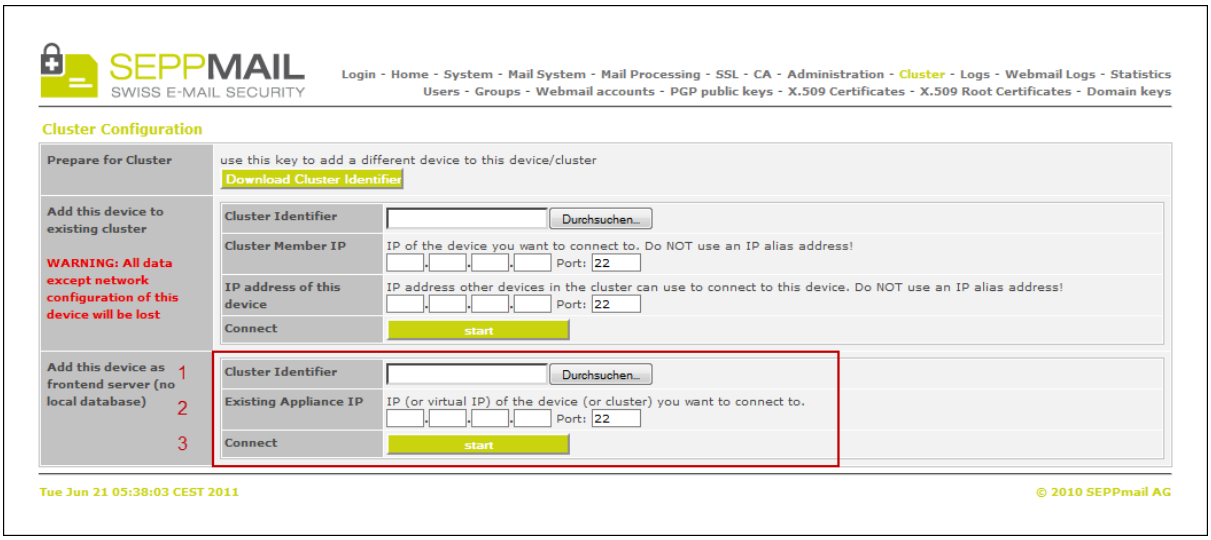

SEPPMAIL
SWISS E-MAIL SECURITY
Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys
Cluster Configuration
Prepare for Cluster
use this key to add a different device to this device/cluster
Download Cluster Identifier
Add this device to existing cluster
WARNING: All data except network configuration of this device will be lost
Cluster Identifier
Durchsuchen...
Cluster Member IP
IP of the device you want to connect to. Do NOT use an IP alias address!
Port: 22
IP address of this device
IP address other devices in the cluster can use to connect to this device. Do NOT use an IP alias address!
Port: 22
Connect
start
Add this device as frontend server (no local database)
1
2
3
Cluster Identifier
Durchsuchen...
Existing Appliance IP
IP (or virtual IP) of the device (or cluster) you want to connect to.
Port: 22
Connect
start
Tue Jun 21 05:38:03 CEST 2011
© 2010 SEPPmail AG

Figure 1. - Adding a SEPPmail appliance as front end server to an existing cluster member system i. e. the cluster compound

© 2014 SEPPmail AG

6.11 "Logs" menu item

Select the »Logs« menu item for managing the email log files and for viewing the log information of the last 500 Email movements. The last email movements are displayed in the »Mail Log (last 500)« section.

Sections	Description
Other Logs	Displaying additional log files
Queue Control	Displaying the email queue, processing the current email queue
Log Archive	Downloading and deleting log files
Filter	Searching in existing log files
Mail Log (last 500)	Displaying the last 500 log entries in the email log file

»Other Logs« section

»Show webmail log...« button

Displaying the log information for the messages, that were sent via GINA technology.

»Show Blacklist / Greylist Log...« button

Displaying the log information for incoming emails that have been fully or temporarily rejected trough greylisting by blacklists rating.

»Queue Control« section

Viewing email messages in the queue 147

»Show queued mails...« button

Select the »Show queued mails...« button, to indicate which emails are currently still in the queue.

»Retry to deliver queued mails...« button

Select the »Retry to deliver queued mails...« button to trigger the sending of emails in the queue.

»Log Archive« section

»Download complete log« button

Select the »Download complete log« button to view the entire email log file. In the current email log file. All current and archived log information is included.

»Download log archive« button

© 2014 SEPPmail AG

Select the »Download log archive« button to view all archived log information.

»Delete log archive« button

Select the »Delete log archive« button to delete the log archive.

»Filter« section

In this input field, enter the values according to which the log files are to be searched. As a result, you get an overview of the log information corresponding to the input filter values.

In addition, select the »Include recently archived logs« option to include the recently archived log information in the search.

To apply the filter to all archived log files, select the »Include complete archived logs (might be time-consuming)« option. It may take some time to display the result depending on the size of the archived log files.

»Mail log (last 500)« section

In this section you can view the log file entries for the last 500 email movements. This is the fastest and most common way to see web log information.

Color code for the current processing status of an email:

black : the email has not been processed or sent directly.
green : the email was successfully delivered.
yellow : the email could not be successfully delivered, this process will be repeated at intervals.
red : the email could not be delivered and was rejected.

You can see the processing status of an email in the column »To« (recipient email address). The recipient email address is represented according to the color codes listed above. This gives you very quick way to recognize the possibility of variations in the processing of incoming and outgoing emails.

The last email movements are displayed with the following details:

Parameter	Description
No.	A consecutive numbering of the email messages. The value of this column is shown in color and also serves as a link to the detailed view of the log information. Select this link and you can view the entire log information for this email.
Source IP	IP address of the email sender. The IP address can identify the email server that has sent the email directly to SEPPmail. (The respective workstation is not meant here.)
Date	Send date of the email
From	Sender's email address

© 2014 SEPPmail AG

Parameter	Description
To	Recipient's email address
Message-ID	Unique identifier of the email
Subject	Subject line of the respective email
Size	Size of the email

6.11.1 Viewing email messages in the queue

»Logs« menu

Emails that are currently in the local SEPPmail email queue (Mail-Queue), can be displayed by clicking the »Show queued mails...« button.

Parameter	Description
ID	Unique identifier of the respective message
Date	Date on which the corresponding email was sent
Size	Size of the email
From	Sender's email address
To	Recipient's email address
Status	The current status of the email processing

© 2014 SEPPmail AG

6.12 "Statistics" menu item

»Statistics« menu

In the overview, the statistics for throughput, technology, antispam, processor and memory statistics are displayed. These statistics are displayed for the time periods Today, Last Week, Last Month, Last year and the last 3 years.

»Throughput Visualisation« section

You can view the number of sent and received messages and the number of performed encryption and decryption operations. You can also view the number of messages, that were processed on average, and how large the maximum number of processed messages per minute was in the corresponding observation period.

Parameter	Description
Today	Throughput statistics for the following time period: today
Last Week	Throughput statistics for the following time period: last week
Last Month	Throughput statistics for the following time period: last month
Last Year	Throughput statistics for the following time period: last year
Last 3 Years	Throughput statistics for the following time period: last 3 years

»Technology Visualisation« section

You can view the number of processed emails separated by the types Secure Webmail, MIME, OpenPGP encryption and domain encryption. You also can view the number of messages processed in average, and how large the maximum number of processed messages per minute was in the corresponding observation period.

Parameter	Description
Today	Technology statistics for the following period: today
Last Week	Technology statistics for the following period: last week
Last Month	Technology statistics for the following period: last month
Last Year	Technology statistics for the following period: last year
Last 3 Years	Technology statistics for the following period: last 3 years

»Spam Visualisation« section

You can view the number of received messages, the number of spam detections and the number of

© 2014 SEPPmail AG

emails, that have been treated based on Black or Grey listing. You can also view the number of spam messages, that were processed on average, and what was the maximum number of processed SPAM messages per minute in the corresponding observation period.

Parameter	Description
Today	SPAM statistics for the following time period: today
Last Week	SPAM statistics for the following time period: last week
Last Month	SPAM statistics for the following time period: last month
Last Year	SPAM statistics for the following time period: last year
Last 3 Years	SPAM statistics for the following time period: last 3 years

»CPU Usage Visualization« section

You can view the CPU usage separately for system processing, processing in user mode (running applications) and processes with respect to the process priority, that have been controlled by the nice utility.

Parameter	Description
Today	Statistics on processor utilization for the following time period: today
Last Week	Statistics on processor utilization for the following time period: last week
Last Month	Statistics on processor utilization for the following time period: last month
Last Year	Statistics on processor utilization for the following time period: last year
Last 3 Years	Statistics on processor utilization for the following time period: last 3 years

»Memory Usage Visualisation« section

You can view the active and total memory usage, memory swapping and free capacity of the working memory.

Parameter	Description
Today	Memory statistics for the following time period: today
Last Week	Memory statistics for the following time period: last week

© 2014 SEPPmail AG

Parameter	Description
Last Month	Memory statistics for the following time period: last month
Last Year	Memory statistics for the following time period: last year
Last 3 Years	Memory statistics for the following time period: last 3 years

© 2014 SEPPmail AG

6.13 "Users" menu item

Select the »Users« menu item to manage the internal users of the SEPPmail appliance.

Following procedures are described in the chapters hereafter:

Overview 151
Creating users 151
Managing users 152

6.13.1 Overview of the "Users" menu item

Parameter	Description
User ID	Name of the user account to log on to the SEPPmail configuration interface.
Name	Actual user name, Robert Lander, for example
Email	Email address of the user
PGP	Number of PGP user keys installed in the user account
S/MIME	Number of S/MIME user certificates installed in the user account
State	Current administrative status of the user

6.13.2 Creating internal user

»Users« menu

To create a new user account, select the »Create new user account...« button.

Fill out the following fields to create the user:

Parameter	Description
User ID	User ID
Full Name	Full name of the user
Email	Email address of the user
Password	Password of the user

»User ID« parameter

Enter in this field the user ID of the user, e.g. the email address or any other unique value. This ID

© 2014 SEPPmail AG

is required to log into the configuration interface.

»Full Name« parameter

Full name of the user, Robert Lander, for example

Note:

Enter the full name of the user, which is mandatory, since this value is required when creating user certificates.

»Email« parameter

Enter in this field the user's email address. On the basis of this email address it will be checked whether a sender is authorized to use crypt function of SEPPmail. The crypto function is not applied to any senders, who do not have a user account.

»Password« parameter

Enter in this field the user's password (enter it twice).

Note:

A password for the user is required only, when this administrative permission is required to get access to the configuration interface. The authorization for access to certain menu items can be defined by selecting the groups.

6.13.3 Managing Internal Users

»Users« menu

To edit the details of a user, click on the »User ID« of the corresponding user.

»User Data« section

Parameter	Description
User ID	Unique user ID
Full Name	The user's full name (editable)
Email	The user's email address (must be unique)
Password	Password of the user
Encryption Settings	Administrative status of the user account
Notification Settings	Read receipt for GINA messages

© 2014 SEPPmail AG

Parameter	Description
User Statistics	Statistical overview of the system use

»User ID« parameter

User ID of the user, e.g. the email address or some other unique value. This parameter is read-only and cannot be changed later. The user ID is the user's login name to access the configuration interface.

»Full Name« parameter

Full name of the user. This parameter can be subsequently changed.

Note:

Enter the mandatory full name of the user, since this value is required, when you create user certificates.

»E-Mail« parameter

User's email address. This parameter is read-only and cannot be changed later.

»Password« parameter

The user's password can be reassigned here.

Note:
A password for the user is required only, when this administrative permission is needed to get to the configuration interface. The authorization for access to certain menu items can be defined by selecting the groups.

»Encryption Settings« parameter

You can influence the administrative status of the user account. You can restrict the user's cryptic functions through the following options, or unlock.

1. May not encrypt mails : disables the encryption of outgoing emails for this user
2. May not sign mails : disables the signing of outgoing emails for this user

If you enable both options, then the user account is disabled. The user can no longer use the cryptic functions, in this case, for outgoing emails. Incoming emails will continue to be decrypted. By disabling the user account, that is maintained in the configuration, but it will not consume any user license.

© 2014 SEPPmail AG

Note:

If a user does not any more require cryptic functions from SEPPmail and S/MIME or OpenPGP keying material no longer exists for that user, we not recommend to delete the user account, but only disable. The used user license becomes free again. Incoming emails for this user can still be decrypted.

If you delete the user account with the existing keying material, such a consumed user license is also released. Incoming email for this user can no longer be decrypted by SEPPmail. The user certificate, for example, of a retired employee may continue to be available and can also be used for encryption of external communication partners.

»Notification Settings« parameter

If sending of notifications is enabled, when sent from this user GINA, emails have been read by the recipient. This refers to all GINA emails sent to this user. The request for a read receipt is then no longer separately required at each outgoing GINA emails. This parameter can be overridden by a higher priority setting within the email domain.

»User Statistics« parameter

Displays a statistical overview of email processed regarding the cryptic method, the number of and the last activity.

»Group Memberships« section

Indicates in which groups the user account is a member. Group membership is managed in the »Groups« menu.

»S/MIME« section

Button/Parameter	Description
Import S/MIME Certificate...	Import existing S/MIME certificate
Generate S/MIME Certificate...	Generates new S/MIME certificate for the user to self generate by the SEPPmail CA
Generate [CA] Certificate...	Refers new S/MIME certificate for the user of the established CA connector
Serial	Serial number of the certificate
Certificate Authority	Subject of the CA, which issued this certificate
Issued on	Date of issue of the certificate
Expires on	Expiry date of the certificate

»PGP« section

© 2014 SEPPmail AG

Button/Parameter	Description
Import PGP key...	Import existing PGP keypair
Generate new PGP key...	Generate new PGP key pair for the user to SEPPmail itself
Key ID	Key ID of the key pair
User ID	User ID of the key pair
Issued on	Date of issue of the keypair
Expires on	Expiration date of the key pair

»Remote POP3« section

Enter the user's POP3 authentication details to regularly retrieve the user's emails from a POP3 server.

Parameter	Description
User ID	User name
Password	Password
Mail server	IP address or host name of the POP3 email server to be picked up by the emails

© 2014 SEPPmail AG

6.14 "Groups" menu item

Select the »Groups« menu item to manage the group structure of the SEPPmail appliance.

Following procedures are described in the sections hereafter:

Overview 156
Creating groups 158
Managing groups 158
Assigning and remove users 158

6.14.1 Overview of the "Groups" menu item

If you also want to give the »admin« user additional administrative rights on the configuration interface, you can make a user a member of different groups. The group structure essentially corresponds to the individual menu items.

Through the »Groups« menu item you have an overview of all the users associated with each group.

An exception is the following group:

»backup (Backup Operator)«. It does not provide for the allocation of privileges to menu items on the configuration interface.

Groups	Description
	Choose the »Create new user group...« button, to create a new group. See Creating groups 158. Groups that were once created, cannot be subsequently deleted.
admin (Administrator)	All members of this group are equal to the default »admin« user and have full administrative access to the configuration interface with full privileges. To add a user to make security equivalent to the default »admin« user, add this user to the »admin (Administrator)« group.
administrationadmin (GUI Access to Administration Section)	All members of this group have access to the »Administration« menu in the configuration interface.
backup (Backup Operator)	This group is assigned with a special meaning. It differs from the system groups for access to the configuration interface by the fact, that there is no access to the configuration interface. All members of this group will receive the system backup of each system once a day via email. The system backup is created every day at 0.00 o'clock and sent via email to all members of this group.
caadmin (GUI Access to CA Section)	All members of this group have access to the »CA« menu in the configuration interface.
clusteradmin (GUI Access to Cluster Section)	All members of this group have access to the »Cluster« menu in the configuration interface.

© 2014 SEPPmail AG

Groups	Description
domainkeysadmin (GUI Access to Domain Keys Section)	All members of this group have access to the »Domain keys« menu in the configuration interface.
groupsadmin (GUI Access to Groups Section)	All members of this group have access to the »Groups« menu in the configuration interface.
homeadmin (GUI Access to Home Section)	All members of this group have access to the »Home« menu in the configuration interface.
logsadmin (GUI Access to Logs Section)	All members of this group have access to the »Logs« menu in the configuration interface.
mailprocessingadmin (GUI Access to Mail Mail Processing Section)	All members of this group have access to the »Mail Processing« menu in the configuration interface.
mailsystemadmin (GUI Access to Mail System Section)	All members of this group have access to the »Mail System« menu in the configuration interface.
multiplecustomersadmin (Admin access to Customer settings in multitenant deployments)	All members of this group have access to the »Customers« menu in the configuration interface.
pgpkeysadmin (GUI Access to PGP Keys Section)	All members of this group have access to the »PGP public keys« menu in the configuration interface.
ssladmin (GUI Access to SSL Section)	All members of this group have access to the »SSL« menu in the configuration interface.
statisticsadmin (GUI Access to Statistics Section)	All members of this group have access to the »Statistics« menu in the configuration interface. In addition, all members of this group receive a daily system report of the respective system. The system report is generated daily at 0.00 o'clock and sent via email to all members of this group.
systemadmin (GUI Access to System Section)	All members of this group have access to the »System« menu in the configuration interface.
usersadmin (GUI Access to Users Section)	All members of this group have access to the »Users« menu in the configuration interface.
webmailaccountsadmin (GUI Access to Webmail Accounts Section)	All members of this group have access to the »Webmail accounts« menu in the configuration interface.

© 2014 SEPPmail AG

Groups	Description
x509certificatesadmin (GUI Access to X.509 Certificates Section)	All members of this group have access to the »X.509 Certificates« menu in the configuration interface.
x509rootcertificatesadmin (GUI Access to X.509 Root Certificates Section)	All members of this group have access to the »X.509 Root Certificates« menu in the configuration interface.

6.14.2 Creating groups

»Groups« menu

To create a new group, select in the configuration interface the »Create new user group...« button. Enter the name of the new group and a brief description and then select the »Create« button, to complete the creation of the new group.

6.14.3 Managing groups

»Groups« menu

Users can be assigned according to the role of one or more groups.

All members of the »backup« group (Backup Operator)« receive the system backup of each system once a day via email. The system backup is created every day at 0.00 o'clock and sent via email to all members of this group. (See chapter Creating a Backup User 23).

The other predefined groups allow their members the administration of the SEPPmail appliance. The »webmailaccountsadmin« group, for example, allows the access to the »Webmail accounts« menu item in the SEPPmail configuration interface.

For each menu item in the configuration interface, there is a corresponding group, each marked with »GUI Access to...«. Thus, various administration tasks can be passed on to multiple people.

To delete an existing group, select the »Edit ...« button next to the group you want to delete. To delete, press the »Delete Group« button.

6.14.4 Assigning and removing users

»Groups« menu

To add a user to an existing group, select the button »Edit...« next to the group to which you want to add a user.

Select in the the pane »Group members« a user. Add this user to the group by the selecting the »Add user...« button. To save the added user, select the »Save changes« button.

To remove a user from a group, select the user entry in the list »Group members« and choose to

© 2014 SEPPmail AG

remove the »Remove selected users...« button.

© 2014 SEPPmail AG

6.15 "GINA accounts" menu item

Select the »GINA Accounts« menu item, to manage the automatically generated web mail accounts of the SEPPmail appliance.

Following procedures are described in the chapters hereafter:

Overview 160
GINA user accounts 162
GINA user accounts 162
Managing GINAuser accounts 162

6.15.1 Overview of the "GINA accounts" menu item

»GINA accounts« menu

This menu is divided in several areas, which are generated partially dynamically. Dynamically generated means in this context, that an own section is displayed for each created customer in the »Customer« menu. All to the customer assigned GINA user accounts will be displayed in this section.

Parameter	Description
[Customer name]	Grouping for one or more customers areas, where to the customer assigned GINA user accounts are grouped.
Default Customer	GINA user accounts, that are not assigned to any other customer
No Customer	GINA user accounts that may not be used
Email	Recipient's email address
Account status	Administrative Status of the GINA user account
Last message status	Status of the last user interaction with time stamp

»[Customer name]« parameter

If a SEPPmail system is used for multiple customers simultaneously, customer-specific configuration parameters may be explicitly assigned. This is also the case for GINA user accounts. For every customer created in the »Customer« menu, there is a special section created, which is referred to with the customer name. Within this custom space, all the customer associated GINA user accounts will be displayed. An external GINA user can be assigned to several customers sections.

»Default Customer« parameter

This section has a special meaning. It contains all the GINA user accounts, that are not assigned to other customers sections.

»No Customer« parameter

© 2014 SEPPmail AG

This section has a special meaning. It contains all the GINA user accounts, that may no longer be used. These GINA user accounts are disabled, but remain in the configuration. They can be reactivated again by assigning them to another customer or the »Default Customer«.

»Email« parameter

Email address of the GINA recipient

»Account status« parameter

Administrative Status of the GINA user account of the recipient. The »Account status« can show the following values:

locked	The GINA account of the recipient is locked.
enabled	The GINA user account of the recipient is active.

»Last message status« parameter

This column displays the status of the last user interaction. The »last message status« can show the following values:

<status message>	If a status message is displayed in red, then the last user interaction was not successfully executed, such as user's log in to the GINA user account.

Examples:

May 2 18:00:00: auth failure, pwdCount 4	The user password of the recipient was entered incorrectly 4 times.
May 2 18:00:00: auth failure, disable account	The user account of the recipient was locked after the user password was incorrectly entered 4 times.

<status message>	If the status message is displayed in green, then the last user interaction was successfully executed, such as reading a GINA message.

Examples:

May 2 18:00:00: success. message-ID: <4DA69716.8030601@customer.com>	A GINA message was successfully decoded and displayed by the recipient.
May 2 18:00:00: auth ok	The recipient was able to successfully log on to the respective GINA user account.

© 2014 SEPPmail AG

6.15.2 Blocking GINA user accounts

»GINA accounts« menu

To lock GINA user accounts, click in the configuration interface on the »GINA accounts« menu item. Then click on the email address of the corresponding GINA user. To lock the selected GINA user account, select in the »User Data« section »Account status« the »locked« option. The user account is now locked, and can only be unlocked by an administrator.

6.15.3 Removing GINA user accounts

»GINA accounts« menu

To GINA delete user accounts, click in the configuration interface on the »GINA accounts« menu item. Then click on the email address of the GINA user. To delete the selected user account, click the »Delete Account« button.

Important note:

When creating a GINA user account, a unique key for encryption and decryption of GINA messages is generated.

All GINA messages for this recipient will be encrypted with the key associated to this GINA user account and can only be decrypted and read again only with this key.

If a GINA user account is deleted, the unique key is also deleted for this user account. This has the consequence, that the recipient cannot decrypt and read all previously received GINA messages.

If a new GINA user account is created for a previously deleted recipient, a new unique key is generated. The recipient can only GINA decrypt and read messages encrypted with the new key. All GINA messages, that have been received before the time of creation of the new GINA user account, can no longer be decrypted and read. This is regardless of whether a newly created GINA user account has the same name as a previously deleted GINA user account.

6.15.4 Managing GINA user accounts

»GINA accounts« menu

»User Data« section

Parameter	Description
Creation Info	Sender's email address and time stamp for creating the GINA user account.
Name	Name of the GINA recipient.
Email	Email address of the recipient.

© 2014 SEPPmail AG

Parameter	Description
Password reminder	Security question in case of loss of the user password. Question and answer these to identify the recipient.
Answer	Answer to the security question.
Password	Setting a new user password.
Must Change Password	If you set this option, the GINA recipient will be prompted to change the password at the next login.
Zip Attachment	GINA messages are sent in a ZIP file attachment.
Account status	Status of the user account.
Password Security Level	
Mobile number	Mobile number of the recipient

»Creation Info« parameter

Sender's email address and timestamp, when creating the GINA user account.

»Name« parameter

Name of the GINA recipient. The recipients can self manage this information within their own GINA user accounts.

»Email« parameter

Email address of the recipient.

»Password reminder« parameter

Security question in case of loss of the user password. Question and answer these to identify the recipient.

»Answer« parameter

Answer to the security question.

»Password« parameter

Setting a new user password.

»Must Change Password« parameter

If you set this option, will the GINA recipient be prompted to change the password at the next login.

»Zip Attachment« parameter

© 2014 SEPPmail AG

Use this parameter, if you want that GINA messages are sent in a ZIP file format on GINA message. This parameter is required for recipients who use Outlook Web Access (OWA), since GINA messages in HTML file format from OWA cannot be decrypted. To use the setting only for individual GINAmessages, can the »[owa]« tag be used in the subject line of the email. If a GINA message arrive in the HTML file format to an OWA recipient, the SEPPmail appliance recognizes this. The sender will then be asked to send the email again. At the same time, the GINA user account of the recipient is automatically set with the »ZIP Attachment« parameter. For all resent GINA messages the GINA messages will be sent in ZIP file format and can be displayed via Outlook Web Access.

»Account status« parameter

locked	Webmail account is disabled/locked
enabled	Webmail account is activated

This option is used in order to avoid Brute-Force* attacks. The GINA user account is automatically disabled after the password has been incorrectly entered 4 times. The user account is locked until it is released by the administrator.

»Password Security Level« parameter

Select the method for password reset, so that external GINA users can reset their GINA user password. Thereafter, depending on the selected method for password reset, one of the following methods is used:

»default (Reset by hotline)« selection value

The »default« value refers to the respective GINA domain selected global default. This is set within the configuration GINA domain in the »Security« section.

»Reset by Email verification« selection value

The external GINA users can reset their password themselves. To activate and confirm the action, they receive an email notification with an activation link. After confirming this external user activation link, the newly entered user password is enabled. A login with the newly set password is now possible.

»Reset by hotline« selection value

The external GINAusers cannot reset their password automatically. They give for that purpose their phone number, under which they can be contacted for support. After review by the security question, they receive a new one-time password from the support staff for next login. After logging in, it is necessary to record a new personal password. A login with the newly set password is now possible.

»Reset by hotline, no reminder question/answer« selection value

The external GINA users cannot reset their password automatically. They give for that purpose their phone number, on which they can be contacted for support. A review by answering a security question is not required. When initializing the first time GINA user account does not require, that the user specifies a security question. The user receives a new one-time password from the support staff for next login. After logging in, it is necessary to record a new personal password. A login with the newly set password is now possible.

These following options for a password reset can be performed only within the »Self Service Password Management (SSPM)« function. See GINA Self Service Password Management 80

© 2014 SEPPmail AG

»Reset by SMS« selection value

The external GINA users can request a new password via SMS to their mobile phone. This new one-time password is used by the user for the next login. After this, they must record a new personal password. A login with the newly set password is now possible.

When resetting the password via SMS, the mobile phone number must have been stored in the user profile of the user.

Including in a selected method for password reset, the SMS option, it is also required that the set up of SMS transmission is done in the »Mail Processing« menu.

»Let user choose between hotline and SMS« selection value

The external GINA users may choose to request a new password from the two options »Hotline« and »SMS«.

»Mobile Number« parameter

Includes the GINA user mobile telephone numbers, if stored by users, when managing their accounts. There is the possibility to the users, for support purposes, if necessary, to send a new one-time password (OTP) as SMS. Click on the »SMS password reset« button. A new automatically generated one-time password is sent through SEPPmail via SMS.

»User Logs« section

In this area you can see a history of user interactions.

* A Brute-Force attack mean searching though all possible (or at least very many) password combinations.

© 2014 SEPPmail AG

6.16 "PGP public keys" menu item

Select the »PGP public keys« menu item, to manage OpenPGP user keys of communication partners on the SEPPmail appliance.

Following procedures are described in the sections hereafter:

Overview 166
Importing OpenPGP key 166
Downloading or deleting OpenPGP key 166

6.16.1 Overview of the "PGP public keys" menu item

Parameter	Description
Key ID	Key ID of the key pair
Email addresses	User ID of the key pair
User Name	Username within the key pair
Issued on	Date of issue of the keypair
Expires on	Expiration date of the key pair

6.16.2 Importing OpenPGP key

»PGP public keys« menu

To import an existing OpenPGP key pair, click the »Import PGP key...« button. When importing an OpenPGP key, you can select the file or insert the key in text form.

6.16.3 Downloading or deleting OpenPGP key

»PGP public keys« menu

To downloador to delete a public OpenPGP key from the SEPPmail appliance to your PC, click on the »Key ID« of the key. To download the OpenPGP key, select the »Download public key« button. If you would like to delete the OpenPGP key, choose the »Delete Key« button. You can also enter a comment about the PGP public key in the Comment field.

© 2014 SEPPmail AG

6.17 "X.509 Certificates" menu item

Select the »X.509 Certificates« menu item, to manage the S/MIME user certificates of the communication partner on the SEPPmail appliance.

Following procedures are described in the sections hereafter:

Overview 167
Importing S/MIME keys 167
Downloading and deleting S/MIME private key 168

6.17.1 Overview of the "X.509 Certificates" menu item

Parameter	Description
Email Address	Email address in the certificate
Certificate Subject	Identification of the certificate
Serial Number	Serial number of the certificate
Issued on	Date of issue of the certificate
Expires on	Expiry date of the certificate

6.17.2 Importing S/MIME user certificate

»X.509 Certificates« menu

Importing manually

To import an existing S/MIME user certificate, click the »Import S/MIME Certificate...« button. Select an S/MIME user certificate to import from the appropriate file. The import file should not be secured with a password.

Importing automatically

Apart from manually importing X.509 user certificates (S/MIME signatures), these can also be imported automatically. For this reason, all incoming S/MIME signed emails are evaluated and checked for quantity of installed and as »trusted« classified root CA certificates. If an S/MIME signature is issued by a trusted root CA, this signature is created in the local certificate store. This signature (public key) is then globally available for all users and can be used to encrypt outgoing emails.

The automated importing of X.509 user certificates (S/MIME signatures) is a basic function of SEPPmail.

© 2014 SEPPmail AG

6.17.3 Downloading or deleting S/MIME user certificate

»X.509 Certificates« menu

To download an S/MIME user certificate from the SEPPmail to your PC, click on the email address of the certificate. To download the S/MIME user certificate, select the »Download Certificate« button. If you want to delete the S/MIME user certificate, select the »Delete Certificate« button.

© 2014 SEPPmail AG

6.18 "X.509 Root Certificates" menu item

Choose the »X.509 Root Certificates« menu item, to manage X.509 root CA certificate of trusted CAs on the SEPPmail appliance.

Following procedures are described in the sections hereafter:

Overview 169
Importing X.509 root certificates 170
Downloading and deleting X.509 root certificates 170
Trusting X.509 root certificates 171

6.18.1 Overview of the "X.509 Root Certificates" menu item

The SEPPmail appliance includes already in delivery condition an extensive list of X.509 root certificates. This list includes the most common public CAs. In productive operation, however, it may be necessary to extend this list with your own X.509 root certificates of communication partners or to delete imported X.509 root certificates.

Parameter	Description
Trust State	current trust status of the certificate
Issued to	Issued to
Issued by	Issued by
Expires on	Expires on

»Trust State« parameter

Trust status of the certificate. There are the following possible values:

? (undefined)	The Trust status »?« (undefined) is assigned for all X.509 root certificates, that the SEPPmail automatically »harvests« from signed inbound S/MIME emails and imports into the certificate store. Since these X.509 root certificates are not yet known, it is necessary, that the use is authorized by an administrator. Note: All newly imported X.509 root certificates that have been assigned with the »?« status (undefined), are listed in the daily status report, which is sent via email to all users of the group »statisticsadmin« at midnight.
trusted	The »trusted« trust status is used for all assigned X.509 root certificates, that will be used for the productive certificate validation of all incoming signed emails.
untrusted	The trust status »untrusted« is awarded for all X.509 root certificates, that are not used for productive certificate check of all incoming signed emails.

© 2014 SEPPmail AG

Note:

The identifiers of the column »Trust State« are displayed in color and serve as a link to view the detailed information of the respective certificate. If you want to display detailed information for each certificate in this menu item, select the identifier of the »Trust State« with the mouse from the corresponding certificate.

»Issued to« parameter

This value usually describes in X.509 root certificates the operator (company) of the root CA or describes the specific use of an intermediate certificate.

»Issued by« parameter

This value in X.509 root certificates usually describes the company or the operator of the root CA, who issued this certificate.

»Expires on« parameter - Validity period

The expiration date of each certificate defines the end of the use of the respective certificate. After reaching i.e. exceeding the expiry date, this certificate is no longer used for certificate verification and email signature. Import a new X.509 root certificate of this CA, if these continue to be used.

6.18.2 Importing X.509 root certificates

»X.509 Root Certificates« menu

Importing manually

To import an existing X.509 root certificate, select the »Import S/MIME Root Certificate« button in the configuration interface. Select to import an X.509 root certificate from the appropriate file.

Importing automatically

Apart from manually importing X.509 root certificates, they can also be imported automatically. For this, all incoming S/MIME signed emails are evaluated. If an S/MIME signature issued by a root CA, that is not located in the certificate store of SEPPmail, it will be automatically imported with the S/MIME signature including the root CA certificate. This automatically imported root CA certificate will be stored in the certificate store marked with the trust status »?« (undefined). None of root CA certificates with this trust status will be used for the verification of S/MIME signatures.

To activate this certificate, it is necessary to set the trust status to the value »trusted«. The presence of an auto-imported root CA certificate with the trust status »?« (undefined), is reported in the daily status report sent to »statisticsadmin« via email.

6.18.3 Downloading and deleting X.509 root certificates

»X.509 Root Certificates« menu

Choose from the list of X.509 root certificates (first column) the link of the certificate, that you want to edit.

© 2014 SEPPmail AG

To download an X.509 root certificate from the SEPPmail appliance on your PC, select the »Download Certificate« button. To delete an X.509 root certificate, select the »Delete Certificate« button.

6.18.4 Trusting X.509 root certificates

»X.509 Root Certificates« menu

To change the trust status of existing X.509 root certificates, click on an untrusted X.509 root certificate in the »Trust State« column, the »UNTRUSTED« link. You can trust the X.509 root certificate by clicking on the »Trust this certificate« button. After you have trusted X.509 root certificate, you will receive the confirmation message »Trust status changed« and that the certificate has the new status »trusted«. Additionally, you can enter a comment to the »Root CA Certificate« in the »Record comment« field.

Similarly, change the trust status to »untrusted«.

6.18.5 Automatically importing X.509 root certificates

»X.509 Root Certificates« menu

The manual import of X.509 root certificates is described in chapter Importing X.509 root certificates. 170 SEPPmail offers the possibility to automatically import yet unknown X.509 root certificates from incoming S/MIME signed emails. This function is also referred to as »Certificate harvesting«.

These automatically imported X.509 root certificates always get the status (Trust State) »undefined«. In the configuration interface of this status is indicated by a »?« question mark. The administrator is notified of newly imported X.509 root certificates in daily system report.

The administrator must manually change the trust status in the configuration interface. Please check before changing the trust status of the new X.509 root certificate for authenticity.

In order to trust a new auto-imported X.509 root certificate, select in the configuration interface the »X.509 Root Certificates« menu item. Then click on an unfamiliar X.509 root certificate in the column Trust State on the »?« link.

To change the trust status, proceed as described in the chapter »Trusting X.509 Root Certificate« 171.

© 2014 SEPPmail AG

6.19 "Domain keys" menu item

Select the »Domain keys« menu item, to manage the OpenPGP domain key and S/MIME domain certificates of the communications partner of the SEPPmail appliance.

Following procedures are described in the chapters hereafter:

Overview 172
Importing OpenPGP domain keys 173
Downloading or deleting OpenPGP domain keys 173
Importing S/MIME domain keys 174
Downloading or deleting S/MIME domain keys 174
Managing domain keys 174

6.19.1 Overview of the "Domain Keys" menu item

The SEPPmail appliance offers the ability to automatically import S/MIME domain certificates from other SEPPmail systems. The import of these S/MIME public domain keys via a central update service is provided by the SEPPmail AG.

When an email domain is set up via the SEPPmail configuration interface, an S/MIME domain certificate is automatically set up depending on the setting. The public part of the certificate (public key) is automatically forwarded to a central update service SEPPmail AG and, after manual examination, automatically distributed to all installed SEPPmail systems worldwide.

»PGP Domain Keys« section

Button/Parameter	Description
Import PGP key...	Button to manually import existing OpenPGP domain certificates from communication partners
Mail Domain	to the domain public key associated with email domain
Key ID	Key ID of the OpenPGP public key
Issued on	Issued by
Expires on	Expiry date of the certificate

»SMIME Domain Certificates« section

Button/Parameter	Description
Import S/MIME certificate...	Button to manually import existing S/MIME domain certificates from communication partners
Mail Domain	to the domain public key associated with email domain

© 2014 SEPPmail AG

Button/Parameter	Description
Email Address	Email address in the domain certificate, such as domain-confidentiality-authority@customer.com
Serial Number	Serial number of the domain certificate
Issued on	Issued by
Expires on	Expiry date of the certificate

»Managed Domain keys« section

Button/Parameter	Description
Update status	Last update attempt of the domain certificates from the central update service
Update domain certificates...	Button to manually perform update of the domain certificates from the central update service
Auto-Update SMIME Domain Certificates	Activates/deactivates the automatic updating of S/MIME domain certificates
Search Domain Certificate...	Search for an existing S/MIME domain certificates in the local domain certificate store for automatically imported Managed Domain Certificates

If you do not want automatic update of the S/MIME domain keys, disable the option »Auto-Update SMIME Domain Certificates«.

6.19.2 Importing OpenPGP domain keys

»Domain keys« menu

To import an existing OpenPGP key pair you choose in the configuration interface the »Import PGP Key...« button. Enter in the »Domain name« field the associated email domain name. You can then select the appropriate file, or insert the key in text form.

6.19.3 Downloading or deleting OpenPGP domain keys

»Domain keys« menu

To download an OpenPGP domain key from the SEPPmail appliance to your PC , click the name of the displayed »E-Mail Domain« of the corresponding key and then click the »Download public key« button. If you, however, would like to delete an OpenPGP domain key, choose the »Delete Key« button.

© 2014 SEPPmail AG

6.19.4 Importing S/MIME domain keys

»Domain keys« menu

To import an existing S/MIME domain certificate, select the »Import S/MIME certificate...« button in the configuration interface. Enter in the »Domain name« field the corresponding email domain name and choose to import the appropriate file of an S/MIME domain certificate.

6.19.5 Downloading or deleting S/MIME domain keys

»Domain keys« menu

To download an existing S/MIME domain certificate from the SEPPmail appliance to your PC, click the name of the displayed »E-Mail-Domain« of the corresponding key and then click the button »Download Certificate«. If you would like to delete an existing S/MIME domain certificate, select the »Delete Certificate« button.

6.19.6 Managing domain keys

»Domain keys« menu

Select the »Update domain certificates...« button, to synchronize domain certificates from other SEPPmail appliances with the own SEPPmail appliance. This adjustment takes place automatically at periodic intervals, if the check box »Auto-Update SMIME Domain Certificates« is enabled.

If you would like to check, whether a specific domain certificate already exists and view its details, enter the appropriate email domain name in the search box and click the button »Search Domain Certificate...«.

© 2014 SEPPmail AG

6.20 "Customers" menu item

Select the »Customers« menu item, to allow the creation of a customized configuration. To use this function, an additional paid license is required.

Following procedures are described in the sections hereafter:

Creating new users 176
Managing existing customers 176
Deleting existing customers 178

General information

If you have the »Multitenancy« function activated, then the email data flow between sender and recipient changes as follows:

- Emails are only transmitted between those senders and receivers, that are assigned to the same customer.
- If a GINA recipient is not assigned by customer as the sender, then a new GINA user account is created among the customers in which also the sender is assigned.
- In the GINA portal registered users can only send messages to the internal recipients, that are assigned to the same customer.
- All S/MIME certificates and PGP key pairs for the same email address will be shared with all GINA user accounts, that also have the same email address.

Each client is exclusively assigned to one or more managed email domains. A managed email domain cannot be assigned to multiple customers. Users of email addresses whose domain has been assigned to a customer, are also automatically assigned to the same customer. Other users can be assigned manually to a customer. GINA recipient must always be assigned to a customer manually

GINA user accounts and managed email domains can only be assigned to a single customer at the same time. No customers explicitly assigned to GINA user accounts and managed email domains are assigned to the »Default Customer«.

Do not assign the same GINA domain to any managed email domains, that is assigned to a customer, other than the GINA domain itself!

© 2014 SEPPmail AG

Each customer may have one or multiple users assigned as special customer administrators. These assigned customer administrators manage the customer assigned GINA user accounts and the GINA domains associated with the managed email domains of the customer.

If the »Multitenancy« function is activated for the first time, then the »Default Customer« is generated. All managed email domains, user accounts and GINA user accounts created at this time, are assigned as »Default Customer«. The system continues operating as before.

Only if customers are created, and these customer managed email domains, customer administrators, GINA user accounts (optional) and user accounts are assigned, will the behavior in the processing of emails change from the previously described.

The special customer »No Customer« is also generated automatically when the »Multitenancy« function is activated for the first time. These customers should all have GINA user accounts assigned, that would otherwise not be assigned to customers. These GINA user accounts should not be used.

6.20.1 Creating new customers

»Customers« menu

Click the »Create new customer...« button in the configuration interface to create a new customer.

»Customer details« section

Parameter	Description
Customer	Name of the customer (not later editable)
Customer Name	Identifier of the customer (later editable)
Customer Admin Email	Email addresses of the customer administrator (later editable)
Comment	Comment (later editable)
Creation info	Information to generate the customer, user with time stamp

»Import backup« section

Import a previously generated customer backup. It is automatically created for a new customer.

6.20.2 Managing existing customers

»Customers« menu

To manage an existing customer, select the customer and click in the configuration interface the »Edit...« button.

Managing a manually created customer or the default customer »Default Customer«

© 2014 SEPPmail AG

»Customer details« section

In this section you can view and alter the detailed data, that you entered when creating the customer.

»Customer administrators« section

In this section you can view and alter the detailed data, that you entered when creating the customer.

»Assigned managed domains« section

In this section you can assign existing managed email domains of this customer.

»Assigned GINA accounts« section

In this section you can add or remove existing GINA user accounts to this customer.

»Backup/Restore« section

»Download« button

Create manually a backup to save a password protected data backup on the local PC.

»Change Password« button

Change the password for the backup. Before you perform the first backup, set the password to protect the backup file.

Note that the backup file is protected with the password, that was current at the time of the creation of the backup.

»Import Backup File« button

Import a previously created backup. All you need, is the password with which the backup file was backed up at the time of the creation. Without the right password, the backup cannot be restored.

Custom language variants for the GINA subsystem are not part of the backup and must be manually backed up and reinstalled.

Managing the special customer »No Customer«

The customer »No Customer« is a special customer. The management of this customers is basically analogous to manually created customer or the »Default Customer« with the following exceptions:

- It cannot be assigned to managed email domains
- No backup can be created for it

© 2014 SEPPmail AG

6.20.3 Deleting existing customers

»Customers« menu

To delete an existing customer, select the customer and click the »Delete…« button in the configuration interface.

When deleting, all to the customer assigned GINA user accounts and managed email domains will be assigned to the »Default Customer«

© 2014 SEPPmail AG

7 Reference of the set of rules statements

7.1 Control structures - if/else statements

The `if/else` statements are control structures and serve within the rulesets to the control flow. They are a fundamental part of the rules. If a condition is met, an action is executed, otherwise an alternative action is executed. The action to be performed, can only be one command. If multiple commands are to be executed as an action, such individual commands can be summarized in a statement block. A statement block is written within curly braces.

Using `if` determines which conditions are to be satisfied to perform an action. With `else`, an alternative action is initiated, if the required `if` condition is not satisfied. An `if/else` statement do not have to be terminated by a semicolon. `if/else` statements can be nested.

Structure of the command

```
if (condition) {
   statement block 1;
}
```

or

```
if (condition) {
   statement block 1;
} else {
   statement block 2;
}
```

The `if` statement determines reason on the return value of the `condition` for the further course in the program sequence. The condition consists of a single instruction, which has at least one return value.

`Statement block 1` is executed only, when the result is positive. Otherwise, if present, only the `statement block 2` is executed.

Example:

```
if (authenticated()) {
} else {
   createaccount('@CREATEGPGKEYS@');
   log(1, 'user account generated');
}
```

Explanation:

The example evaluates the return value of the command `authenticated()`. If the internal internal

© 2014 SEPPmail AG

sender of the email is successfully authenticated, the return value is true, and then proceeding in the program sequence continues without further action. If the authentication was not successful, a user account is created for the sender.

7.2 General commands

Parameters, which are shown in square brackets, e.g. [OLDRECIPIENT] are optional and do not need to be specified. If not specified, a predefined default value or default behavior is applied.

The following variables are available inside the templates:

Variable	Description
$header_from	From header
$from	From
$header_to	To header
$to	To
$header_cc	CC
$mailid	Message ID
$subject	Subject

7.2.1 add_rcpt()

The command `add_rcpt()` makes it possible to add an additional recipient email address.

Structure of the command

```
add_rcpt('email address');
```

The command must be terminated by a semicolon.

This command is used to add an additional recipient email address. The email address is added to the envelope.

The return value is always positive. This command has one parameter.

»Email address« parameter

This parameter defines an email address that is added as an additional recipient in the envelope.

Example:

© 2014 SEPPmail AG

```
add_rcpt('recipient@customer.org');
```

Explanation:

In this example, an additional recipient is added. At the recipient, the email appears in the inbox as, if it was sent via BCC. The original recipient will not be changed.

7.2.2 authenticated()

The command `authenticated()` checks the identification status of the sender of the email. The identification status of the sender comprises the identity and authentication.

Structure of the command

```
authenticated(['header']);
```

The command must be terminated by a semicolon. The return value of this command is positive, if the sender has been successfully authenticated, otherwise negative. This command has one parameter.

Note:

Authenticated means, that either the user has been authenticated via SMTP, or that the email comes from an email server that has a relay authority. The relay authority is added in the menu »Mail System« -> section »Relaying«.

As a user, the locals Named User will be designated on the appliance.

»header« parameter

If `header` is specified as a value, the user will be re-authenticated. In addition, the email address of the header's `FROM` field is used.

Example 1:

```
if (authenticated()) {
} else {
   createaccount('@CREATEGPGKEYS@');
   log(1, 'user account generated');
}
```

Explanation:

This example evaluates the return value of the `authenticated()`. If the internal sender of the email is successfully authenticated, the return value is true, and operation proceeds without further action in the program sequence. If the authentication was not successful, a user account is created for the sender.

© 2014 SEPPmail AG

Example 2:

```
if (authenticated(['header'])) {
} else {
   createaccount('@CREATEGPGKEYS@');
   log(1, 'user account generated');
}
```

Explanation:

This example evaluates the return value of the command `authenticated()`. If the internal sender of the email is successfully authenticated, the return value is true, and operation proceeds without further action in the program sequence. If the authentication was not successful, a user account is created for the sender.

7.2.3 compare()

The command `compare()` compares values in header fields.

Structure of the command

```
compare('Header field', 'Operator', 'Value');
```

The command must be terminated by a semicolon.

This command compares the contents of the `header field` parameter with help of the `operator` parameter with the `value` parameter.

The return value of this command is positive, if the parameter `value` occurs at least once, otherwise negative. This command has three parameters.

»Header field« parameter

Specifies the `header field`, whose content is to be compared against the contents of the parameter's `value`. All headers in an email can be used as header fields.

Examples of the »Header field« parameter:

- return-path
- from
- to
- subject
- envelope-to
- etc..

»Operator« parameter

`equal` : compares for equality

© 2014 SEPPmail AG

`match` : checks analogy of a regular expression

`substitute` : is the same as `match`, but removes the relevant part of `value` from `header field`

Note:

Coded fields are decoded before comparison. The special characters tabulator, carriage return, line feed and line end are removed before comparison with the `equal` operator.

»Value« parameter

Specifies the value to compare against. This value can also be a regular expression.

Example 1:

```
compare('x-smenc', 'equal', 'yes');
```

Explanation:

This example checks, if the header field `x-smenc` includes exactly the value 'yes'. This does not mean, that only the value of 'yes' exists, but that the value 'yes' is included.

Example 2:

```
if (compare('to', 'match', '\@customer\.com')) {
   tagsubject('[nosign]');
} else {}
```

Explanation:

This example checks for an outgoing email in the header field `to` with the operator `match` for the presence of the domain '@customer.com' within the recipient's email address. If the recipient's email address contains the string '@customer.com', then the return value from `compare()` is true, the tag '[nosign]' is added in the subject. Depending on the basic configuration of the ruleset, this means, that this email is not signed.

Example 3:

```
compare('subject', 'substitute', '(\s)*\[secure\]');
```

Explanation:

This example checks the subject, header field `subject`, of an email for the presence of the regular expression '(\s)*\[secure\]'. This expression is evaluated in the string '[secure]'. If this string is found within the subject, it is removed.

© 2014 SEPPmail AG

7.2.4 compareattr()

The `compareattr()` command makes it possible to examine attributes / system variables.

Structure of the command

```
compareattr('Attribute', 'Operator', 'Value');
```

The command must be terminated by a semicolon.

This command compares, with the help from the `operator`, the content of the `header field` with the `value`.

The return value is positive, provided that at least one occurrence exists, otherwise negative. The command has three parameters.

»Attribute« parameter

`Attribute` can address the variable `connect_from` or variables that have been written with `ldap_read()` or `setuserattr()`.

»Operator« parameter

The `operator` has two different operators to choose from:

`equal` : compare identity.
`match` : checked for analogy of a regular expression.

»Value« parameter

Value to be compared against.

Example:

```
if (compareattr('connect_from','equal','172.16.161.1')) {
     log(1,'Message comes from 172.16.161.1'); }
else {
     log(1,'Message does NOT come from 172.16.161.1');
}
```

Explanation:

In this example, it is examined, whether the email to be processed is coming from server specified in an email server. It is evaluated against the system variable `connect_from`.

© 2014 SEPPmail AG

7.2.5 comparebody()

The command `comparebody()` makes it possible to search through an email for a specified value.

Structure of the command

```
comparebody('Value');
```

The command must be terminated by a semicolon.

This command searches the message body of an email for the specified `value`.

The return value of this command is positive, if the parameter `value` occurs at least once, otherwise negative. This command has one parameter.

»Value« parameter

The `Value` parameter defines the search term, that will be sought for in the email. `Value` has the format of a regular expression.

Example:

```
if (comparebody('(\d{1,3}\.){3}\d{1,3}')) {
     log(1, 'Mail contains an IP address');
} else {
     log(1, 'Mail does not contain an IP address');
}
```

Explanation:

In this example, the message body of an email is examined for an IP address. If at least one IP address is found, the log entry 'Mail contains an IP address' is written in the system logger. If no IP address is found, the log entry 'Mail does not contain an IP address' is written in the system logger.

7.2.6 disclaimer()

The command `disclaimer()` adds a text attachment to an existing email.

Structure of the command

```
disclaimer(['Template'], ['Position'], ['force']);
```

The command must be terminated by a semicolon.

This command adds a text attachment from the `template` of an existing email. If an empty string is specified as a `template`, an attempt is made using the options of the "Managed Domains" to choose the correct disclaimer. For this purpose, the respective email domains associated disclaimers are evaluated.

© 2014 SEPPmail AG

If `force` is set to `true`, then each outgoing email is added to a text attachment. This is regardless of whether or not it is in a reply email. If `force` is not specified, then the »Also add disclaimer to replies (in-reply-to header set)« parameter and »Add disclaimer to all outgoing emails« in the »Mail Processing« menu -> »Ruleset Generator« section -> pane -> »General Settings« are evaluated. Instead of `true`, also `yes` or `1` can be used.

The return value is always positive. This command has three parameters.

»Template« parameter

Defines the name of the template which is to be used as a text attachment. Templates can be managed in the »Mail Processing« menu -> »Edit Disclaimer« section.

»Position« parameter

`top` : above the email body
`bottom` : under the email body

`Default` : bottom

»force« parameter

This parameter will force adding a text attachment to an outgoing email.

Option to »force« parameter

Possible values: `true` or `yes` or `1`

Example:

```
disclaimer('', 'bottom', 'yes');
```

Explanation:

In this example, the default text attachment is selected using the options within the »Managed Domains« and appended to the end of every email. It does not matter whether or not it is a reply email.

7.2.7 from_managed_domain()

The command `from_managed_domain()` makes it possible to check, if an email was sent from a sender of a »Managed Domain«.

Structure of the command

```
from_managed_domain();
```

The command must be terminated by a semicolon.

© 2014 SEPPmail AG

The return value is positive, if the email was sent from a sender of a »Managed Domain«, otherwise negative.

The command has no parameters.

Example:

```
if (from_managed_domain()) {
     log('1', 'Email is from managed domain');
} else {
     log('1', "Email isn't from managed domain");
}
```

Explanation:

In this example, it is checked whether an email was sent from an email address registered under »Managed Domains«.

7.2.8 incoming()

The command incoming `incoming()` makes it possible to determine the delivery destination of an email.

Structure of the command

```
incoming();
```

The command must be terminated by a semicolon.

This command verifies, if an email is delivered locally. If all the recipients of the email are not exclusively local or exclusively non-local, two groups are formed.

Note:

The delivery of an email exclusive locally means, that this email can be forwarded to a recipient who has been defined under »Managed Domains«. Email to these recipients are viewed as exclusively local recipients and treated by the `statement block 1`.

The delivery of an email not exclusively locally means, that the email will be forwarded to an external recipient. This email will be treated as an outgoing email and handled by the `statement block 2`.

The return value is positive for the group of local recipients. For the group of non-local recipients, the return value is negative. This command has no parameters.

Example:

```
if (incoming()) {
     .
     Ruleset statements for all emails that can be locally delivered
     .
```

© 2014 SEPPmail AG

```
     Statement block 1 - Return value: positive
     .
} else {
     .
     Ruleset statements for all emails, that cannot be locally delivered
     .
     Statement block 2 - Return value: negative
}
```

Explanation:

In this example, the `statement block 1` is executed for an incoming email. For an outgoing email the `statement block 2` is executed.

7.2.9 log()

The command `log()` makes it possible to record a message in the syslog.

Structure of the command

```
log ('step', 'entry');
```

The command must be terminated by a semicolon.

This command sends the value of the `entry` parameter in the system logger. An identifier (message ID) is attached to the entry in parentheses. The value of the `step` parameter can take a value from 0 to 7, and determines the importance of the entry.

The recorded log messages can be viewed in the »Logs« menu.

The return value is always positive. This command has two parameters.

»Step« parameter

n	Significance	n	Significance
0	Debug	4	Error
1	Info	5	Critical
2	Notice	6	Alert
3	Warning	7	Emerg

»Entry« parameter

Enter the text that is to be recorded as a log entry in syslog.

Example:

© 2014 SEPPmail AG

```
log ('1', 'Hello World');
```

Header of the email:

```
Date: Fri, 05 Aug 2013 11:40:00 +0200
From: sender@customer.com
To: recipient@customer.de
Subject: Some Topic
Content-Type: text/plain;
Message-Id: <E0D4DE42-DCB5-11D7>
```

Recording in the log:

```
Aug 05 11:40:04 test gateway: <E0D4DE42-DCB5-11D7> Hello World
```

Explanation:

The string 'Hello World' is recorded with the `info` priority in the syslog.

7.2.10 logheader()

The command `logheader()` makes it possible to send the contents of a header to the system logger.

Structure of the command

```
logheader('HEADER');
```

The command must be terminated by a semicolon.

This command is used for debugging the processing of email through the RuleEngine. It is sent to the content of the `HEADER` in the system logger.

The return value is always positive. This command has no parameters.

Example:

```
logheader('Message-ID');
```

Explanation:

In this example, the contents of the 'Message-ID' header is sent in the system logger.

© 2014 SEPPmail AG

7.2.11 normalize_header()

The command `normalize_header()` makes it possible to replace all special characters in a header by normal ASCII characters.

Structure of the command

```
normalize_header('HEADER');
```

The command must be terminated by a semicolon.

This command replaces all special characters in `HEADER` by normal ASCII characters. Special characters can be, for example, German umlauts like ä, ö, ü or?.

The return value of this command is always positive. This command has one parameter.

»header« parameter

Specifies the name of the `HEADER`.

Examples of the »HEADER« parameter:

- return-path
- from
- to
- subject
- envelope-to
- etc..

Example 1:

```
normalize_header('subject');
```

Explanation:

In this example, the header field of the `subject` string 'Herr Müller' becomes in the normalized form as 'Herr Mueller'.

Example 2:

```
normalize_header('to');
```

Explanation:

In this example, the header field in the `to` string '<Bernd Hänsel> bernd.haensel@customer.com' becomes in normalized form '<Bernd Haensel> bernd.haensel@customer.com'.

© 2014 SEPPmail AG

7.2.12 notify()

The command `notify()` makes it possible to send an email notification regarding an email processed by SEPPmail.

Structure of the command

```
notify('recipient address', 'Template', ['From: "System Admin"
<admin@securemail.com>;X-MyHeader: Test']);
```

The command must be terminated by a semicolon.

This command generates an email notification and sends it to the `recipient address`.

The `recipient address` can, beside an email address also, be the `sender` variable for sender email address or the `admin` variable for the email address of the local administrator.

The appearance of the email is defined by the `template`.

The third parameter allows you to insert additional own header. Several headers can be separated with » ; «.

The return value is always positive. This command has three parameters.

»Recipient address« parameter

This parameter may include the following values:

recipient@customer.com : email address, e.g. robert.lander@customer.com

Variables

`sender` : represents the sender address of the processed original email
`admin` : represents the email address of the local SEPPmail administrator

Note:

The placeholder `admin` refers to the local administrator of the appliance. You define this in the »Mail System« menu -> »SMTP settings« section -> »Postmaster address« parameter.

»Template« parameter

Defines the appearance and content of the email notification. Templates can be managed in the »Mail Processing« menu -> »Edit Disclaimer« section.

»Own Header« parameter

This parameter allows you to define and attach your own header. Several headers can be separated by a semicolon » ; «.

Example of own header:

© 2014 SEPPmail AG

From : "System Admin" <admin@customer.com>
X-MyHeader : MyOwnHeaderValue

Summarized notation of the parameter with multiple additional headers:

'From: "System Admin" <admin@customer.com>;X-MyHeader: MyOwnHeaderValue'

The subject of an email, defined by the `Subject` header, cannot be changed. This value is always `Notification` and is fixed.

Example 1:

```
notify('sender', 'bounce_noenc', 'From: "System Admin"
<admin@securemail.com>;X-MyHeader: Test');
```

Explanation:

When processing an email, an additional email notification is generated. This is sent to the sender of the processed email. The email address of the sender is available above the variable `sender`. As message content, the content of the template `bounce_noenc` is used. There the `From` header and `X-MyHeader` are inserted in addition with the respective values.

Example 2:

```
notify('revision@customer.com', 'monit_rev', 'From: "System Admin"
<admin@customer.com>;X-MyHeader: Revision');
```

Explanation:

When processing an email, an additional email notification is generated. This is sent to the email address `revision@customer.com`. As message content, the content of the template `monit_rev` is used. There the `From` header and `X-MyHeader` are inserted in addition to the respective values.

7.2.13 replace_rcpt()

The command `replace_rcpt()` makes it possible to change the recipient of an email.

Structure of the command

```
replace_rcpt(['OLDRECIPIENT'], 'NEWRECIPIENT');
```

The command must be terminated by a semicolon.

The recipient of the processed email may be changed depending on the parameters used. Each parameter corresponds to a regular expression, that must provide an email address as a result of an email address or a part of an email address. If the value for the parameter OLDRECIPIENT of the value

© 2014 SEPPmail AG

'admin@customer.com' it is assumed, that this is the original recipient in the email, and ' support@customer.com' is defined for the value of the parameter, and then the email is sent to the new recipient 'support@customer.com'.

Also parts of the two parameters can be described as a regular expression. It can, for example, search for the domain portion within the parameter and this will be replaced by a new value.

Multiple recipients can be separated with » ; « semicolons.

The return value is always positive. This command has two parameters.

»OLDRECIPIENT« parameter

Regular expression, that describes the original email address or any part thereof.

»NEWRECIPIENT« parameter

Regular expression, that describes the new email address or any part thereof.

Example:

```
replace_rcpt('\@mydomain\.com', '\@customer\.ch');
```

Explanation:

In this example, the parameter `OLDRECIPIENT` of the domain portion of the original email address of the recipient of the '@mydomain.com' in the value of the parameter `NEWRECIPIENT`, '@customer.ch', is changed. The part of the email address before the '@' remains thus unchanged. If `OLDRECIPIENT` is specified, only this recipient or the part of the recipient is adjusted.

If more than one email recipient addresses are present, all the recipient addresses of '@mydomain.com' to '@mydomain.ch' would be changed.

7.2.14 replace_sender()

The command replace_sender() allows you to change the sender in the envelope of an email.

Structure of the command

```
replace_sender('new sender', ['subst']);
```

The command must be terminated by a semicolon.

This command replaces the original sender of an email in the envelope by `new_sender`. The value for `From` is not changed. The `subst` parameter corresponds to a regular expression. If `subst` is specified, that to `subst` corresponding part of the original sender is replaced by the value of `new_sender`.

The return value is always positive. This command has two parameters.

© 2014 SEPPmail AG

»new sender« parameter

This parameter is the value by which the original sender email address is replaced in the envelope. If `subst` is specified, the `new_sender` character string, that is used for the part of the email address, is applied to the `subst`.

»subst« parameter

Regular expression, that is applied to the original sender email address.

Example 1:

```
replace_sender('new_sender@customer.com');
```

Explanation:

In this example, the email address in the envelope of the email, is replaced by ' new_sender@customer.com'.

Example 2:

```
replace_sender('@customer.com', '\@customer\.org');
```

Explanation:

In this example, the part of the email address in the envelope of the email will be replaced though the regular expression '\@customer\.org' applied through '@customer.com'.

7.2.15 rmatch()

The command `rmatch()` makes it possible to check, if a regular expression applies to all recipients.

Structure of the command

```
rmatch('REGEXP');
```

The command must be terminated by a semicolon.

The return value of this command is positive, if the email was successfully tested to contain `REGEXP` , otherwise negative. This command has one parameter.

»REGEXP« parameter

Defines the regular expression to be tested for.

Example 1:

© 2014 SEPPmail AG

```
if (rmatch('\@customer\.org')) {
     notify ('sender', 'info_send_email');
} else {}
```

Explanation:

In this example, it is checked whether the email address of all recipients of an email, has the domain component '@customer.org'. If this is the case, then an email notification is sent to the sender.

Example 2:

```
if (rmatch('\@customer\.org')) {
     notify ('sender', 'info_send_email', 'From: "System Admin"
<admin@customer.com>');
} else {}
```

Explanation:

In this example, it is checked whether the email address of all recipients of an email, have the domain component '@customer.org'. If this is the case, then an email notification is sent to the sender. In addition, a new value is set to the `From` header.

7.2.16 rmatchsplit()

The command `rmatchsplit()` makes it possible to split an email with a regular informal term.

Structure of the command

```
rmatchsplit('REGEXP');
```

The command must be terminated by a semicolon.

The regular expression is applied to the entire email. This includes all the headers and the entire body of the email. An email will be divided into several groups, if it was successfully tested for the regular expression. A group that matches the regular informal term and another group, that does not match the regular expression. By the regular expression can also a plurality of groups be generated. The command `rmatchsplit()` is classically used within the `if/else` control structure.

The return value of this command is positive, if the email was successfully tested to contain `REGEXP` , otherwise negative. This command has one parameter.

»REGEXP« parameter

This parameter defines the regular expression, for which the email is checked.

Example:

```
if (rmatchsplit('sales@customer\.com|Invoice')) {
```

© 2014 SEPPmail AG

```
     log(1, 'regex test successful');
} else {
     log(1, 'regex test not successful');
}
```

Explanation:

In this example, the email is checked for the presence of the text components `sales@customer.com` or `Invoice`. If one of these textual elements is found within the entire email, then the statement `log(1, 'regex test successful')` is executed, otherwise the statement `log(1, 'regex test not successful')` is executed.

7.2.17 rmheader()

The command `rmheader()` makes it possible to delete a header line in an email.

Structure of the command

```
rmheader('HEADER');
```

The command must be terminated by a semicolon.

Note:

If multiple headers with the name `HEADER` exist, all headers are deleted.

Deletes the header line specified with `HEADER` in the email.

The return value is always positive. The command has one parameter.

»Header« parameter

Specifies the header field, that is to be deleted.

Examples of the »Header field« parameter:

- return-path
- from
- to
- subject
- envelope-to
- etc..

Example:

```
rmheader('X-Greylist');
```

© 2014 SEPPmail AG

Explanation:

In this example, all `X-Greylist` headers are removed.

7.2.18 setheader()

The command `setheader()` makes it possible to add or to change a header line in an email.

Structure of the command

```
setheader('HEADER', 'TEXT');
```

The command must be terminated by a semicolon.

This command adds an email a `HEADER` with a `VALUE`. If this header already exists, it will be changed to the specified `VALUE`.

Note:

If multiple headers with the name `HEADER` exist, the first respective header found is adapted.

The return value is always positive. This command has two parameters.

»Header« parameter

Indicates the header field, which is to be added or changed.

Examples of the parameter »Header field«:

- return-path
- from
- to
- subject
- envelope-to
- etc..

Example 1:

```
setheader('x-smenc','yes');
```

Explanation:

In this example, an additional `x-smenc` header with the value 'yes' is added to an email.

Example 2:

© 2014 SEPPmail AG

```
setheader('from','info@customer.com');
```

Explanation:

In this example, the `from` header field in an email is changed to the value 'info@customer.com'.

7.2.19 logsubject()

The command `logsubject()` makes it possible to monitor the contents of the subject line of an email.

Structure of the command

```
logsubject();
```

The command must be terminated by a semicolon.

This command sends the contents of the subject line as log info to the system logger.

The return value is always positive. This command has no parameters.

7.2.20 tagsubject()

The command `tagsubject()` makes it possible to attach to the subject of an email a text component.

Structure of the command

```
tagsubject('TEXT');
```

The command must be terminated by a semicolon.

The specified `TEXT` is to be added in the subject line of an email.

The return value is always positive. This command has one parameter.

»TEXT« parameter

The parameter specifies the text (character string), which is appended to the subject line.

Example:

```
tagsubject('[priv]');
```

Explanation:

© 2014 SEPPmail AG

In this example, the string '[priv]' will be appended to the contents of the subject line of an email.

© 2014 SEPPmail AG

7.3 User management commands

7.3.1 createaccount()

The command `createaccount()` makes it possible to create new user accounts.

Structure of the command

```
createaccount(['KEYS'],['USERID'],['NAME']);
```

The command must be terminated by a semicolon.

A local user account SEPPmail is designated as user account. This account can be found in the »Users« menu. This command is classically used within an LDAP connection for user management.

The return value of this command is always positive. This command has three parameters.

»KEYS« parameter

This parameter specifies which keying material is to be generated automatically, when creating the user account. Formatted according to a bit mask in octal notation.

The following values are available:

Bit 0 : generate OpenPGP key pair
Bit 1 : generate S/MIME certificate with own CA
Bit 2 : generate S/MIME certificate via CA Connector

	Mask	Mask	Mask	Mask	Mask
Bit 0: OpenPGP	x	x	x		
Bit 1: S/MIME with own CA		x			x
Bit 2: S/MIME via CA connector			x	x	
Value for `KEYS`	1	3	5	4	2

»USERID« parameter

This parameter specifies the user's UID.

»NAME« parameter

This parameter specifies the user's name.

Note:

- Variables, that were set by `ldap_read()`, can be used for `USERID` and `NAME`.
- Special characters in `USERID` and `NAME` will be automatically replaced.

© 2014 SEPPmail AG

7.3.2 member_of()

The command `member_of()` makes it possible to examine whether sender is associated to a particular group.

Structure of the command

```
member_of('group');
```

The command must be terminated by a semicolon.

A locale SEPPmail group is referred as a group. These groups are managed in the »Groups« menu.

The return value is positive, if the sender is associated with the specified group, otherwise negative . This command has one parameter.

»Group« parameter

Defines the name of the group to which the email address of the sender is to be tested for membership.

Example:

```
if (member_of('support')) {
     setheader('x-smenc','yes');
} else {}
```

Explanation:

In this example, it is tested whether the sender is member of the 'support' group. If yes, the return value is true, and the command `setheader()` is executed. If not, return value will be false.

7.3.3 setuserattr()

The command `setuserattr()` makes it possible to store additional information for the current user.

Structure of the command

```
setuserattr('ATTR', 'VALUE');
```

The command must be terminated by a semicolon.

It will set an additional variable for the current user. The user must be authenticated.

The return value is always positive. The command has two parameters.

© 2014 SEPPmail AG

Note:

- Variables, that have been set through `ldap_read()` for `VALUE`, can be used.
- It can be used for all the attributes of inetOrgPerson.
- The attributes can be displayed in the GUI.

»ATTR« and »VALUE« parameters

The following system attributes are available:

<table>
<tr><th>ATTR</th><th>VALUE</th></tr>
<tr><td>accountOptions</td><td>Bit 0: User must not encrypt
Bit 2: User must not sign

<table><tr><th></th><th>Mark</th><th>Mask</th><th>Mask</th></tr><tr><td>Bit 0: User must not encrypt</td><td>x</td><td></td><td>x</td></tr><tr><td>Bit 1: not assigned</td><td>-</td><td>-</td><td>-</td></tr><tr><td>Bit 2: User must not sign</td><td></td><td>x</td><td>x</td></tr><tr><td>Value for <code>VALUE</code></td><td>1</td><td>4</td><td>5</td></tr></table></td></tr>
<tr><td>Sn</td><td>Name of the user</td></tr>
<tr><td>userPassword</td><td>User's password for GUI access</td></tr>
<tr><td>Uid</td><td>User ID</td></tr>
</table>

© 2014 SEPPmail AG

7.4 Certificate management commands

7.4.1 attachpgpkey()

The command `attachpgpkey()` makes it possible to attach the OpenPGP public key of the sender to an email.

Structure of the command

```
attachpgpkey();
```

The command must be terminated by a semicolon.

This command attaches the OpenPGP public key of the sender of an email as an attachment.

The return value is always positive. The command has no parameters.

7.4.2 has_smime_key()

The command `has_smime_key()` makes it possible to check whether the user has a valid S/MIME private key component.

Structure of the command

```
has_smime_key();
```

The command must be terminated by a semicolon.

The return value is positive, if the user has a valid S/MIME private key component, otherwise negative. The command has no parameters.

Note:

- The return value is negative, when the user's S/MIME certificate has just expired.
- The return value is negative, when the status of the user is set to »may not encrypt«.

7.4.3 smime_create_key()

The command `smime_create_key()` makes it possible to generate an S/MIME certificate for a user.

Structure of the command

```
smime_create_key(['SUBJECT']);
```

© 2014 SEPPmail AG

The command must be terminated by a semicolon.

This command generates an S/MIME certificate for a user by the local CA. Optionally, the `SUBJECT` for the certificate can be specified.

The return value is always positive. The command has one parameter.

»SUBJECT« parameter

Defines the subject for the generated S/MIME certificate.

Within the `SUBJECT`, the variable `$sender` is available. This variable is available for the sender of the email.

Example:

```
smime_create_key('/C=CH/OU=Department/O=Company/emailAddress=$sender');
```

Explanation:

In this example, an S/MIME certificate is generated by the local CA. The optional `SUBJECT` is also given.

7.4.4 smime_revoke_keys()

The command `smime_revoke_keys()` makes it possible to revoke all unexpired S/MIME certificates of a user.

Structure of the command

```
smime_revoke_keys();
```

The command must be terminated by a semicolon.

The return value is positive, if all certificates could be revoked or have expired. The return value is negative, if at least one certificate could not be revoked, e.g. because it is an imported certificate.

This command has no parameters.

7.4.5 swisssign_create_key()

The command `swisssign_create_key()` makes it possible to obtain an S/MIME certificate for a user from the SwissSign certification body.

Structure of the command

```
swisssign_create_key();
```

© 2014 SEPPmail AG

The command must be terminated by a semicolon.

This command has no parameters.

© 2014 SEPPmail AG

7.5 Message handling commands

7.5.1 archive()

The command `archive()` makes it possible to reprocess an email.

Structure of the command

```
archive('EMAIL ADDRESS');
```

The command must be terminated by a semicolon.

The email will be sent within the processing additionally to the `EMAIL ADDRESS`, or the email will add the `EMAIL ADDRESS` as an additional recipient.

The return value is always positive. The command has one parameter.

»EMAIL ADDRESS« parameter

Email address of the additional recipient

Example:

```
archive('recipient@customer.com');
```

Explanation:

In this example, the currently processed email is also sent to the recipient 'recipient@customer.com'.

7.5.2 bounce()

The command `bounce()` makes it possible to refuse the processing of an email.

Structure of the command

```
bounce('Template', 'Header as an attachment');
```

The command must be terminated by a semicolon.

This command generates a »Bounce« email and deletes the original email. The appearance of the »Bounce« email is defined by the `template`. The sender of this email is »admin«. The email will attach the Header of the original email as a file attachment, when `Header attachment` has the Boolean value `true`. Instead of `true`, also `yes` or `1` can be used.

The command has no return value. This command has two parameters.

© 2014 SEPPmail AG

Note:

- All subsequent commands will be ignored.
- This command cannot be the condition of an `if/else` statement (see chapter if/else statements[179]).

»Template« parameter

Defines the template to use. Templates can be managed in the »Mail Processing« menu -> »Edit Disclaimer« section.

»Header as attachment« parameter

Option to the »Header as attachment« parameter

Possible values : `true`, alternatively `yes` or `1`

Example:

```
bounce('bounce', 'yes');
```

Explanation:

Delivery of the email should be denied and an email to be sent to the sender. The content of the email is defined in the bounce template. The email should be attached to the Header of the undelivered email as an attachment. The statement looks like this:

7.5.3 deliver()

The command `deliver()` makes it possible to immediately deliver an email.

Structure of the command

```
deliver(['Mailserver[:Port]'|'loop'|'queueless'|'']);
```

The command must be terminated by a semicolon.

This command delivers the email from the specified email server / port. If no parameter is specified, the email is delivered to the local mail transport agent (MTA).

Note:

- All subsequent commands are ignored.
- This command cannot be the condition of an `if/else` statement (see chapter if/else statements[179]).

The return value is always positive. The parameter has one parameter.

Parameter

© 2014 SEPPmail AG

Options for the parameter

`loop` :	The email is returned to the mail server from which it was assumed.
`queueless` :	This setting causes, that mails are not stored to individual recipients during the processing. Instead, the incoming connection is acknowledged only, if the outgoing connection has been acknowledged. If the assumption for some recipients are not acknowledged, when sending to multiple recipients, these mails stay briefly on the appliance, until it acknowledged by the receiving mail server.
`no option`	The command is called without parameters.

Example 1:

```
deliver('relay.customer.com:587');
```

Explanation:

In this example, the email is sent to the specified email server with the destination port TCP/587.

Example 2:

```
deliver();
```

Explanation:

In this example, the email is delivered directly via its own local mail transport agent (MTA).

7.5.4 drop()

The command `drop()` allows an email to be rejected.

Structure of the command

```
drop(['CODE'], ['ERROR']);
```

The command must be terminated by a semicolon.

This command will cause an email to not be processed, and to optionally return an error code.

The command has no return value. The command has two parameters.

Note:

- Neither a »Bounce« email to the sender nor a message to the recipient is generated.
- All subsequent commands are ignored.
- This command cannot be the condition of an `if/else` statement (see section if/else statements 179).

© 2014 SEPPmail AG

Alternative error codes can also be set using `CODE` and `ERROR`.

If no parameters are specified, the default error code is returned to the corresponding message text.

Default: `CODE` = '555', `ERROR` = 'mail not accepted'

»CODE« parameter

Specifies the error code in the form of a numerical value to, for example, 420

»ERROR« parameter

Returns the error code in the form of a character string, e.g. system temporarily unavailable.

Example:

```
drop('420', 'system temporarily unavailable');
```

Explanation:

The email will be rejected with temporary error »420 system temporarily unavailable«.

7.5.5 reprocess()

The command `reprocess()` makes it possible to reprocess an email.

Structure of the command

```
reprocess();
```

The command must be terminated by a semicolon.

All to an email attached emails are reprocessed and sent back to the sender. This may be necessary, if still encrypted email messages are in a user's inbox. These can be sent to re-decryption to the appliance and might be processed or decrypted.

The command has no return value. This command has no parameters.

Note:

- The original Message-ID is removed from the newly decrypted emails.
- There will be no »Bounce« email created at the sender.
- All subsequent commands will be ignored.
- This command cannot be the condition of an `if/else` statement (see chapter if/else Statements 179).

Example:

© 2014 SEPPmail AG

```
if (compare('to', 'match', '(?i)reprocess\@decrypt\.reprocess')) {
     log(1, 'reprocess recipient found - Re-injecting attached
messages');
     reprocess();
     drop('220', 'message reprocessed');
} else {}
```

Explanation:

In this example, an internal user sends an encrypted email as an attachment in a non-encrypted email to the system-specific email address `reprocess@decrypt.reprocess.` The encrypted email, in the attachment is reprocessed, or the email is attempted to be deciphered. It creates a log entry. After running `reprocess()`, the original email is deleted with `drop()`.

© 2014 SEPPmail AG

7.6 Encryption and decryption commands

7.6.1 decrypt_pgp()

The command `decrypt_pgp()` makes it possible to decrypt PGP-encrypted and signed emails.

Structure of the command

```
decrypt_pgp();
```

The command must be terminated by a semicolon.

This command attempts to decrypt all PGP encrypted and signed texts and attachments of an email and to check their signatures.

The return value is positive, if at least one text or an attachment was decrypted or its signature was successfully verified. Otherwise, the return value is negative. This command has no parameters.

7.6.2 decrypt_domain_pgp()

The command `decrypt_domain_pgp()` makes it possible to decrypt domain encrypted and signed PGP emails.

Structure of the command

```
decrypt_domain_pgp();
```

The command must be terminated by a semicolon.

This command attempts to decrypt all PGP encrypted and signed texts and attachments of an email and to check their signatures, that have been encrypted by the sender via domain encryption.

The return value is positive, if at least one text or an attachment was decrypted or its signature was successfully verified. Otherwise, the return value is negative. This command has no parameters.

7.6.3 domain_pgp_keys_avail()

The command `domain_pgp_keys_avail()` makes it possible to verify the availability of PGP public domain keys.

Structure of the command

```
domain_pgp_keys_avail('Usage');
```

The command must be terminated by a semicolon.

© 2014 SEPPmail AG

This command verifies whether email domain PGP public keys in the local certificate store are available to all recipients.

The return value is positive, if the email domain PGP public keys are available for all recipients present and, if the `usage` parameter value was specified `strict`, otherwise the return value is negative. If the value `auto` is specified for the `usage` parameter, the receivers are divided into two groups. The group of recipients, for whom the domain PGP public keys are available, receives a positive return value. The group of recipients for which no domain PGP public keys are present, receives a negative return value.

The command has one parameter.

7.6.4 decrypt_smime()

The command `decrypt_smime()` makes it possible to decrypt S/MIME encrypted emails.

Structure of the command

```
decrypt_smime();
```

The command must be terminated by a semicolon.

This command attempts to decrypt an S/MIME encrypted email.

The return value is positive, if the email has been decrypted, otherwise negative. This command has no parameters.

7.6.5 decrypt_domain_smime()

The command `decrypt_domain_smime()` makes it possible to decrypt domain encrypted S/MIME emails.

Structure of the command

```
decrypt_domain_smime();
```

The command must be terminated by a semicolon.

This command attempts to decrypt a domain encrypted S/MIME email.

The return value is positive, if the email has been decrypted, otherwise negative. This command has no parameters.

7.6.6 domain_smime_keys_avail()

The command `domain_smime_keys_avail()` makes it possible to check the availability of S/MIME domain public keys.

Structure of the command

© 2014 SEPPmail AG

```
domain_smime_keys_avail('Usage');
```

The command must be terminated by a semicolon.

This command checks if domain S/MIME public keys in the local certificate store are available to all recipients of an email.

The return value is positive, if the email domain S/MIME public keys are available for all recipients and if the value of the `usage` parameter was specified `strict`, otherwise the return value is negative. If the value `auto` is specified for the `Usage` parameter, the receivers are divided into two groups. The group of recipients, for whom the domain S/MIME public keys are available, receives a positive return value. The group of recipients for whom no domain S/MIME public keys are present, receives a negative return value.

The command has one parameter.

7.6.7 delete_smime_sig()

The command `delete_smime_sig()` makes it possible to delete the S/MIME signature of an email.

Structure of the command

```
delete_smime_sig();
```

The command must be terminated by a semicolon.

This command deletes a signature from the signed email.

The return value is positive, if the email was signed by the S/MIME method. Otherwise, the return value is negative. This command has no parameters.

Note:

The validity of the S/MIME signature is not checked.

7.6.8 encrypt_pgp()

The command `encrypt_pgp()` makes it possible to encrypt and to sign emails by PGP.

Structure of the command

```
encrypt_pgp('Signature' [, 'Address']);
```

The command must be terminated by a semicolon.

© 2014 SEPPmail AG

This command encrypts all text and attachments of the email. In addition, they are signed, if the `signature` has the Boolean value `true`. Instead of `true`, also `yes` or `1` can be used. If the `address` is specified, the PGP public key of this recipient is used to encrypt all emails for all recipients exclusively.

If PGP public keys are not available for all recipients, two groups are formed.

The return value is positive for the group of recipients, that could be encrypted. For the group of recipients, that could not be encrypted, the return value is negative. This command has two parameters.

»Signature« parameter

Option of the »Signature« parameter

Possible values: `true` or `yes` or `1`

»Address« parameter

Email address of the recipient, whose PGP public key is to be used for encryption.

Example:

```
encrypt_pgp('yes', 'recipient@customer.org');
```

Explanation:

In this example, it is attempted to encrypt all texts and attachments of an email and to sign as `signature` to value 'yes'. The PGP public key of the specified recipient `address` will be used to encrypt. In our case 'recipient@customer.org'.

7.6.9 encrypt_domain_pgp()

The command `encrypt_domain_pgp()` makes it possible to encrypt emails via PGP domain encryption.

Structure of the command

```
encrypt_domain_pgp();
```

The command must be terminated by a semicolon.

This command encrypts all texts and attachments of the email via PGP domain encryption. If domain PGP public keys are not available for all recipients, two groups are formed.

The return value is positive for the group of recipients that could be encrypted. For the group of recipients that could not be encrypted, the return value is negative. This command has no parameters.

© 2014 SEPPmail AG

Example:

```
encrypt_domain_pgp();
```

Explanation:

In this example, all texts and systems of an email are attempted to be encrypted via PGP domain encryption.

7.6.10 encrypt_smime()

The command `encrypt_smime()` makes it possible to encrypt emails via S/MIME.

Structure of the command

```
encrypt_smime();
```

The command must be terminated by a semicolon.

This command encrypts an email according to the S/MIME standard. If S/MIME certificates are not available for all recipients, two groups are formed.

The return value is positive for the group of recipients that could be encrypted. For the group of recipients that could not be encrypted, it is negative. This command has no parameters.

7.6.11 encrypt_domain_smime()

The command `encrypt_domain_smime()makes` it possible to encrypt emails via S/MIME domain encryption.

Structure of the command

```
encrypt_domain_smime();
```

The command must be terminated by a semicolon.

This command encrypts all text and attachments in email via S/MIME domain encryption. If domain S/MIME public keys are not available for all recipients, two groups are formed.

The return value is positive for the group of recipients that could be encrypted. For the group of recipients that could not be encrypted, the return value is negative. This command has no parameters.

Example:

```
encrypt_domain_smime();
```

© 2014 SEPPmail AG

Explanation:

In this example all texts and systems of an email are attempted to be encrypted via S/MIME domain encryption.

7.6.12 encrypt_webmail()

The command `encrypt_webmail()` makes it possible to encrypt an email using the GINA technology.

Structure of the command

```
encrypt_webmail(['TEMPLATE']);
```

The command must be terminated by a semicolon.

This command encrypts a message via GINA technology for the delivery address. The encrypted message can then be further processed in the RuleEngine.

Recommendation:

The GINA sends the message directly with `deliver()`.

The recipient address is taken from the currently processed message.

If `TEMPLATE` is specified, a special template is used for the GINA message. If not, the template is selected based on the sender address. The template is in this case the applied to GINA profile or applied to the GINA domain called.

The return value is always positive. The command has one parameter.

»TEMPLATE« parameter

Defines the applied GINA profile or the applied GINA domain.

7.6.13 pgp_encrypted()

The command `pgp_encrypted()` makes it possible to check an email for PGP encryption.

Structure of the command

```
pgp_encrypted();
```

The command must be terminated by a semicolon.

This command checks whether the given email is encrypted with the PGP method.

© 2014 SEPPmail AG

The return value is positive, if the email is PGP encrypted, otherwise negative. The command has no parameters.

7.6.14 pgp_keys_avail()

The command `pgp_keys_avail()` makes it possible to check the availability of PGP public keys.

Structure of the command

```
pgp_keys_avail('Usage');
```

The command must be terminated by a semicolon.

This command checks, whether a PGP public key in the local certificate store is available to all recipients of an email.

The return value is positive, if the email PGP public keys are available for all recipients and the `usage` parameter for the application was specified `strict`, otherwise the return value is negative. If the `auto` value specified for the `usage` parameter, the receivers are divided into two groups. The group of recipients, to whom PGP public keys are available, receives a positive return value. The group of receivers, to whom no PGP public keys are available, receives a negative return value.

The command has one parameter.

7.6.15 pgp_secret_keys_avail()

The command `pgp_secret_keys_avail()` makes it possible to check the availability of PGP private keys.

Structure of the command

```
pgp_secret_keys_avail();
```

The command must be terminated by a semicolon.

This command checks, whether a PGP private key is available to all recipients of an email.

The return value is positive, if a PGP private keys is available for the sender, otherwise negative.

This command has no parameters.

7.6.16 smime_keys_avail()

The command `smime_keys_avail()` makes it possible to check the availability of S/MIME public keys.

Structure of the command

© 2014 SEPPmail AG

```
smime_keys_avail('Usage');
```

The command must be terminated by a semicolon.

This command checks, whether S/MIME public keys are available to all recipients of an email in the local certificate store.

The return value is positive, if S/MIME public keys are available to all recipients of the email, and for the `usage` parameter value was specified `strict`, otherwise the return value is negative. If the value `auto` is specified for the `Usage` parameter, the receivers are divided into two groups. The group of recipients, to whom the S/MIME public keys are available for, gets a positive return value. The group of recipients for which no S/MIME public keys are available receives a negative return value.

The command has one parameter.

7.6.17 sign_smime()

The command `sign_smime()` makes it possible to provide an email with the S/MIME signature of the sender.

Structure of the command

```
sign_smime();
```

The command must be terminated by a semicolon.

The return value is positive, if the message is successfully signed, otherwise negative. This command has no parameters.

Example:

```
if (sign_smime()) {
     log(1, 'sign smime successful');
} else { }
```

Explanation:

In this example, an email will be provided with the S/MIME signature of the sender. It is further checked, whether this operation was successfully performed. If so, the return value is `true` and a log info is sent to the system logger.

7.6.18 smime_signed()

The command `smime_signed()` makes it possible to check an email for the presence of an S/MIME signature.

Structure of the command

© 2014 SEPPmail AG

```
smime_signed();
```

The command must be terminated by a semicolon.

This command checks, if the present email is signed with the S/MIME method.

The return value is positive, if the email S/MIME is signed, otherwise negative. This command has no parameters.

7.6.19 smime_encrypted()

The command `smime_encrypted()` makes it possible to check an email for S/MIME encryption.

Structure of the command

```
smime_encrypted();
```

The command must be terminated by a semicolon.

This command checks, whether the present email is encrypted using the S/MIME method.

The return value is positive, if the email is S/MIME encrypted, otherwise negative. This command has no parameters.

7.6.20 validate_smime_sig()

The command `validate_smime_sig()` makes it possible to examine the S/MIME signature of an email for validity.

Structure of the command

```
validate_smime_sig('Store vertificate');
```

The command must be terminated by a semicolon.

This command checks the S/MIME signature of an email for validity. In addition to the signature verification, the certificate can be imported into the certificate store of the appliance, when the `store certificate` parameter value `true` is set. Instead of `true`, also `yes` or `1` can be used.

The return value is positive, if all of the following are true:

- The email was signed with the S/MIME method.
- The email is complete and unchanged.
- The email was signed with an S/MIME certificate, that has been issued by a classified trusted Certificate Authority (CA).
- The S/MIME certificate, that is used to attach the signature, is neither listed on one by the

© 2014 SEPPmail AG

appliance known "revocation list" (CRL), nor has its expiration date is passed.

If any of the above is not true, the return value is negative. This command has one parameter.

»Save certificate« parameter

Option of »Save certificate« parameter

Possible values: `true` or `yes` or `1`

Example:

```
if (validate_smime_sig('true')) {
     log(1, 'smime signed valid');
} else {
     log(1, 'smime signed, but signature invalid');
}
```

Explanation:

In this example, the S/MIME signature of an email will be checked for validity. If the return value from `validate_smime_sig()` is positive, then the log entry 'smime signed valid' is written. Otherwise, the log entry 'smime signed, but signature invalid' is written.

7.6.21 webmail_keys_avail()

The command `webmail_keys_avail()` command allows to check, if a GINA user account is available.

Structure of the command

```
webmail_keys_avail('Usage');
```

The command must be terminated by a semicolon.

This command checks, whether a GINA user account is available to all recipients of an email. If the `Usage` of the command is `strict`, the return value is positive only, if GINA user accounts are available for all recipients. If the Usage is `auto`, the command divides the recipients into two groups and gives each group the appropriate return value.

This command has one parameter.

7.6.22 webmail_keys_gen()

The command `webmail_keys_gen()` makes it possible to create GINA user accounts.

Structure of the command

© 2014 SEPPmail AG

```
webmail_keys_gen(['Recipient address'], ['Password length'],
['NoPwEmailIsSmsSend']);
```

The command must be terminated by a semicolon.

This command generates a GINA user account and sends the initialization password to the sender of the original email or to a `recipient address`, if it is specified.

The return value is always positive. The command has three parameters.

»Recipient address« parameter

Defines the email address, to which the email with the initialization password should be sent.

»Length of the password« parameter

Defines the length of the password: 0 for blank password. If the parameter is not specified, the default value will be used. This can be viewed and changed via the configuration interface.

»NoPwEmailIsSmsSend« parameter

Option of »NoPwEmailIsSmsSend« parameter

Possible values: `true` or `yes` or `1`

Example:

```
webmail_keys_gen('', '8');
```

Explanation:

In this example, a GINA user account is generated. The sender of the original email will receive an email notification with the initialization password. The password for this GINA user account must have at least 8 characters.

7.6.23 pack_mail()

The `pack_mail()` command allows to pack an outgoing email for forwarding to a GINA Relay system.

Structure of the command

```
pack_mail('Email-Addr', ['Domainsignature']);
```

The command must be terminated by a semicolon.

This command packages an email for forwarding to a GINA relay system. Email Addr defines the email address of the GINA relay system. If the optional domain signature parameter is true, the packed email is also signed. Instead of `true`, also `yes` or `1` can be used.

© 2014 SEPPmail AG

The return value is positive if the packing of the email was successful, otherwise negative. The command has two parameters.

»Email-Addr« parameter

Defines the email address of the GINA relay systems

»Domainsignature« parameter

Option for '' »Domainsignature« parameter

Possible values: `true` or `yes` or `1`

Example:

```
pack_mail('gina-relay@customer.org', 'yes');
```

Explanation:

In this example, the outgoing email is packed for forwarding to a GINA relay system. From this, a new email message is generated and sent to the destination email address of the GINA relay system. In addition, this email message is signed with the domain certificate.

7.6.24 unpack_mail()

The command `unpack_mail()` makes it possible to unpack a packed email for a GINA relay system.

Structure of the command

```
unpack_mail();
```

The command must be terminated by a semicolon.

The return value is always positive. This command has no parameters.

© 2014 SEPPmail AG

7.7 LDAP commands (access to external sources)

7.7.1 ldap_compare()

The ldap_compare `ldap_compare()` makes it possible to compare a value stored in an LDAP directory with a specified attribute.

Structure of the command

```
ldap_compare('URI;USER;PASSWORD;BASEDN;FILTER', 'ATTR', 'VALUE');
```

The command must be terminated by a semicolon.

This command establishes a connection to an LDAP server and checks the value of an attribute.

The return value is positive, if `VALUE` is present in the attribute, otherwise negative. This command has three parameters.

Parameter

Parameter	Description
URI	The IP address or the name of the LDAP server. It can be given two comma separated values: In this case, automatic access to the second server, when the first cannot be achieved.
USER	The user, who will be used for accessing
PASSWORD	The password of the user
BASEDN	The base DN (distinguished name) for the query
FILTER	The filter for the query
ATTR	The attribute, which is to be queried
VALUE	The value, which should appear in the attribute

Example:

It should be checked, whether the current user of the group belongs to »My group«.

The statement looks like this:

```
ldap_compare('192.168.10.10;CN=Peter Mueller,OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firm,DC=local;mypassword;OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firm,DC=local;(mail=$sender)','memberOF',Mygroup');
```

Explanation:

© 2014 SEPPmail AG

- If the specified attribute, or the searched entry does not exist, the return value is negative.
- If several entries are found, only the first is evaluated.
- If several attributes are to be found, all attributes are evaluated (multi-value).
- If none of the specified LDAP servers is reachable, the mail is rejected with a temporary error.

7.7.2 ldap_read

The command ldap_read() makes it possible to read a value stored in an LDAP directory.

Structure of the command

```
ldap_read('URI;USER;PASSWORD;BASEDN;FILTER' ,'ATTR', 'VAR');
```

The command must be terminated by a semicolon.

This command establishes a connection to an LDAP server and stores the value of the queried attribute in the variable `VAR`. The return value is positive, if a value can be assigned to the variable `VAR`, otherwise negative. This command has three parameters.

Parameter

Parameter	Description
URI	The IP address or the name of the LDAP server. You can specify two comma separated values: in this case, the second server is automatically accessed, when the first cannot be acquired.
USER	The user, who will use the access
PASSWORD	The password of the user
BASEDN	The Base DN (Distinguished Name) for querying
FILTER	The filter for the query
ATTR	The attribute that is to be retrieved
VAR	Variable in which the attribute is to be stored

Example:

This is the value of the »name« attribute read from an LDAP directory. This is to be stored in the »name« variable.

```
ldap_read('192.168.10.10;CN=Peter Mueller,OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firm,DC=local;mypassword;OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firm,DC=local; (mail=$sender)','name','name'););
```

Explanation:

© 2014 SEPPmail AG

- If the specified attribute or searched entry does not exist, the variable is assigned with an empty value.
- If multiple entries (objects) are found, only the first is evaluated.
- If several attributes are found, all attributes are read and assigned, separated by semicolons ";", to the variable (multi-value attribute).
- If none of the specified LDAP servers is reachable, the mail is rejected with a temporary error.

7.7.3 ldap_getcerts()

The command `ldap_getcerts()` makes it possible to retrieve S/MIME public keys to an LDAP directory service.

Structure of the command

```
ldap_getcerts('URI;USER;PASSWORD;BASEDN');
```

The command must be terminated by a semicolon.

This command makes it possible to request S/MIME public key for each recipient of an email with an LDAP directory service.

The return value is always positive. This command has one parameter.

Parameter

Example:

`URI` : ldap-directory.domain.tld
`USER` : User name for logging on to the LDAP directory
`PASSWORD` : Password to log on to the LDAP directory
`BASEDN` : ou=pki-participant,dc=pki,dc=domain,dc=tld

Parameter	Description
URI	The IP address or the name of the LDAP server. You can specify two comma separated values: in this case, the second server is automatically accessed, when the first cannot be acquired.
USER	The user, who will be used for accessing
PASSWORD	The password of the user
BASEDN	The Base DN (Distinguished Name) for querying

Example:

```
ldap_getcerts('ldap-directory.domain.tld;;;ou=pki-participant,dc=pki,
dc=domain,dc=tld');
```

© 2014 SEPPmail AG

Explanation:

In this example, the S/MIME public key is retrieved with an LDAP directory service for the recipient of an email. Access to this LDAP directory service is public, and therefore no credentials are required.

7.7.4 ldap_getpgpkeys()

The command `ldap_getpgpkeys()` makes it possible to retrieve PGP public keys with an LDAP directory service.

Structure of the command

```
ldap_getpgpkeys('URI;USER;PASSWORD;BASEDN');
```

The command must be terminated by a semicolon.

This command makes it possible to call PGP public key for each recipient of an email with an LDAP directory service.

The return value is always positive. This command has one parameter.

Parameter

Example:

`URI` : ldap-directory.domain.tld
`USER` : User name for logging on to the LDAP directory
`PASSWORD` : Password to log on to the LDAP directory
`BASEDN` : ou=pki-participant,dc=pki,dc=domain,dc=tld

Parameter	Description
URI	The IP address or the name of the LDAP server. It can be specified with two comma separated values: in this case, the second server is automatically accessed, if the first cannot be achieved.
USER	The user, who will be used for accessing
PASSWORD	The password of the user
BASEDN	The Base DN (Distinguished Name) for querying

Example:

```
ldap_getpgpkeys('ldap-directory.domain.tld;;;ou=pki-participant,dc=pki,
dc=domain,dc=tld');
```

Explanation:

© 2014 SEPPmail AG

In this example, the PGP public key for the email recipient is retrieved with an LDAP directory service. Access to this LDAP directory service is public and therefore no credentials are required.

© 2014 SEPPmail AG

7.8 Content management commands

7.8.1 iscalendar()

The command `iscalendar()` makes it possible to check an email for the presence of the mime type »text/calendar«.

Structure of the command

```
iscalendar();
```

The command must be terminated by a semicolon.

The command verifies, whether the email contains the mime type »text/calendar«. If yes, the return value is positive, otherwise negative. This command can be used to prevent emails with calendar entry implications e.g. invitations, appointments, meeting requests becoming signed. Microsoft Outlook cannot, for example, handle signed calendar entries.

This command has no parameters.

7.8.2 isspam()

The command `isspam()` makes it possible to check an email for spam.

Structure of the command

```
isspam('MARKLEVEL', 'TAG', 'REJECTLEVEL');
```

The command must be terminated by a semicolon.

The return value of this command is always positive. This command has three parameters.

»MARKLEVEL« parameter

This parameter defines the threshold value, from which an email will be tagged as spam email. For marking the specified `TAG` will be used.

Range of values : 0.5 - 9.5
Increment : 0.5

»TAG« parameter

This parameter defines a word element (`TAG`) is appended to mark an email as SPAM in the subject.

Example for this parameter: [SPAM]

»REJECTLEVEL« parameter

© 2014 SEPPmail AG

This parameter defines the threshold value from which an email is rejected as SPAM.

Range of values : 0.5 - 9.5
Increment: 0 .5

Example:

```
isspam('2.5', '[SPAM]', '4.5');
```

Explanation:

In this example, an email is checked for SPAM. The parameter for `MARKLEVEL` has the value '2 .5 '. If this threshold is reached or exceeded during the SPAM checking, the email will be tagged with the '[SPAM]' `TAG`. The `TAG` is attached to the subject. If the threshold value '4 .5 'for `REJECTLEVEL` is reached or exceeded, the email is rejected and will not be received.

7.8.3 partoftype()

The command `partoftype()` makes it possible to determine the file type of email file attachments.

Structure of the command

```
partoftype('Type', 'Action', 'Check archive content');
```

The command must be terminated by a semicolon.

This command checks whether the file attachments of an email correspond to a particular `Type`. The `Action` defines, what happens to the data systems, if the test on the `Type` is positive. The contents of archive files are searched when archive `Content check` has the Boolean value `true`. Instead of `true` can also be used `yes` or `1`.

The return value is always positive, if the result of at least one check of the file attachments of an email is positive, otherwise it is negative. The command has three parameters.

»Type« parameter

More information about the parameter `Type` can be found in the section List of file types 231.

»Action« parameter

For the parameters of `Action`, the following options are available:

`info` : provides the result for the following commands at your disposal
`delete` : additionally removes the file attachment from the email

»Check archive contents« parameter

Option of »Check archive contents« parameter

© 2014 SEPPmail AG

Possible values : `true`, alternatively `yes` or `1`

Example:

```
partoftype('EXE', 'delete', 'true');
```

Explanation:

In this example, an email is checked for the presence of attachments of the `type` 'EXE'. If an attachment is found, it is removed from the email. If the email contains an archive file as file attachment, then this is also searched. If the file `Type` 'EXE' is found inside the archive file, the file is removed from the archive.

7.8.4 vscan()

The vscan() command makes it possible to examine all the data assets of an email for viruses.

Structure of the command

```
vscan('Email-Addr-for-notification');
```

The command must be terminated by a semicolon.

This command checks all file attachments of an email for known viruses. If a virus is found, an email notification is sent to `Email-Addr-for-notification`. A subsequent ruleset command must handle this email on.

The return value is always positive, if the result of at least one check of the file attachments of an email is positive, otherwise it is negative. The command has one parameter.

»Email-Addr-for-notification« parameter

Defines the email address, to which a notification of virus detection will be sent.

Example:

```
vscan('antivirus-admin@customer.com');
```

Explanation:

In this example, an email notification is sent to 'antivirus-admin@customer.com', if a virus was found.

© 2014 SEPPmail AG

7.9 File types

7.9.1 List of file types

The following file types can be distinguished:

ID	Description
BMP	PC Bitmap
BZIP	BZIP Compressed
CAB	Microsoft CAB file
COM	MSDOS Computable
EMF	Enhanced Windows Metafile
EXE	MSDOS Executable
FAX	G3 Fax
GIF	GIF Image
GZIP	GZIP Compressed
ICO	Windows Icon
ISO9660	ISO 9660 CD-ROM
JPEG	JPEG Image
JPG2000	JPEG 2000 Image
LHA	LHa 2.x? Archive
LHARC	LHarc 1.x Archive
LWF	LuraWave Image
MPEG.L3	MPEG Layer 3
MPEG.SYS	MPEG System Stream
MPEG.VID	MPEG Video
MS.ASF	Microsoft ASF
MS.OFF	MS Office document
MS.XLS	MS Excel 5.0 Worksheet
NIFF	NIFF Image
PBMPLUS	PBMPLUS Bitmap
PCX	Z-Soft Image
PDF	PDF Document
PNG	PNG Image
RAR	RAR Archive
RIFF.ANI	MS RIFF Animated Cursor
RIFF.AVI	MS RIFF Audio Video Interleave
RIFF.DIB	MS RIFF DIB Bitmap
RIFF.MID	MS RIFF MIDI File
RIFF.MMF	MS RIFF Multimedia Movie
RIFF.WAV	MS RIFF Wave Audio
RTF	Rich Text Format
TAR	TAR Archive

© 2014 SEPPmail AG

ID	Description
TARGA	TARGA Bitmap
TIFF	TIFF Image
ZIP	PKZIP Archive
ZOO	Zoo Archive

List of file types

© 2014 SEPPmail AG

7.9.2 Groups of file types

The following groups of file types can be distinguished:

ID	Description	Contained file types
ARCHIVES	Archive files	ZIP ZIP.SFX RAR LHARC LHA SQUISH UC2 ZOO TAR CAB BZIP GZIP
EXE	Executable files	EXE.PE EXE COM
FS	File systems	ISO9660 HISIERRA
IMAGES	Pictures	JPEG BMP TIFF PNG GIF TARGA PBMPLUS NIFF FAX PCX LWF ICO JPG2000 EMF
MEDIA	Multimedia	RIFF.WAV RIFF.AVI RIFF.ANI RIFF.MID RIFF.MMF RIFF.DIB RIFF RIFX MPEG.VID MPEG.SYS MPEG.L3 MS.ASF
OFFICE	Office documents	RTF PDF MS.OFF MS.XLS

Groups of file types

© 2014 SEPPmail AG